Hossam Nabil El Shenraky *Editor*

Analytical Studies on Cybercrimes Against Children in the Dark Web

Detection and Prevention

Springer

Analytical Studies on Cybercrimes Against Children in the Dark Web

Hossam Nabil El Shenraky
Editor

Analytical Studies on Cybercrimes Against Children in the Dark Web

Detection and Prevention

Springer

Editor
Hossam Nabil El Shenraky
Dubai Police Academy
Dubai, United Arab Emirates

ISBN 978-981-95-8468-0 ISBN 978-981-95-8469-7 (eBook)
https://doi.org/10.1007/978-981-95-8469-7

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

If disposing of this product, please recycle the paper.

Preface

The digital age has brought unparalleled advancements in connectivity, information sharing, and technological innovations. However, alongside these benefits, the internet—especially the dark web—has also become a platform for some of the most heinous crimes, including child sexual exploitation. The anonymity provided by encryption technologies, cryptocurrencies, and decentralized platforms has facilitated illicit activities, making it increasingly challenging for law enforcement agencies, policymakers, and researchers to combat these offenses effectively.

This volume, *Analytical Studies on Cybercrimes Against Children in the Dark Web*, seeks to provide a comprehensive examination of the various dimensions of child exploitation on the dark web. The chapters included herein delve into multiple facets of this crisis, ranging from investigative methodologies and forensic tools to the legal, technological, and psychological challenges associated with combating online child abuse. By drawing on interdisciplinary perspectives, the book offers insights into how artificial intelligence, blockchain forensics, and international collaboration can be leveraged to track and dismantle illicit networks operating within hidden corners of the internet.

The contributions to this volume are authored by leading experts in cybersecurity, law enforcement, criminology, psychology, and digital forensics, each presenting critical analyses and case studies that reflect the evolving nature of cybercrimes against children. Key topics explored include the role of blockchain forensics in tracking illicit cryptocurrency transactions, the effectiveness of international agencies such as Interpol in addressing cyber-exploitation, and the ethical and legal implications of AI-generated child abuse materials. Additionally, the volume discusses the alarming rise of deepfake technology and AI-driven manipulation, shedding light on the risks posed by automated tools that enable offenders to create and distribute harmful content.

One of the primary objectives of this book is to raise awareness among researchers, law enforcement professionals, policymakers, and the general public about the severity and scope of child exploitation crimes on the dark web. By offering research-driven recommendations, this volume aims to inform policy development,

encourage technological innovations in cybercrime detection, and promote stronger international cooperation in the fight against these egregious crimes.

We extend our sincere gratitude to the scholars, practitioners, and institutions that have contributed to this book. Their expertise and dedication to this critical area of research have been instrumental in shaping the discussions presented here. We also acknowledge the tireless efforts of law enforcement agencies and advocacy organizations working to protect children from online harm.

It is our hope that this volume will serve as a valuable resource for those committed to understanding and mitigating the dangers of child exploitation on the dark web. Through collaborative efforts, enhanced technological interventions, and rigorous legal frameworks, we believe that progress can be made in safeguarding the most vulnerable members of our society from digital harm.

Dubai, United Arab Emirates, 2026 Prof. Hossam Nabil El Shenraky

Contents

Investigating Deepfake AI-Generation of CSAM and CSEM (Challenges and Solutions) 1
Hossam Nabil El Shenraky

Investigating Children Sexual Abuse Cases in the Dark Web 25
Eldar Saljic and Dusko Tomic

Blockchain Forensics & Public–Private Alliances: Tackling Child Exploitation on the Dark Web 49
Ahmad Alsuwaidi and Irenee Dondjio

Interpol's Crucial Role in Tackling Child Exploitation on the Dark Web 85
Amer Fakhoury

Using Artificial Intelligence Algorithms to Monitor Child Sexual Exploitation in the Dark Web Environment 95
Amar Yasser El-Bably

The Role of Artificial Intelligence in Committing Child Sexual Abuse on the Darknet: Challenges and Opportunities 133
Hesham Badawy

A Digital Forensics Approach to Investigate Child Exploitation in the Dark Web 163
Ibtesam Mohamed Al Awadhi

The Child Offender and Victim on the Darknet: A Case Study 2 179
Mohammad Elhady Abdelhakiem Ratib Abdelhafiz

Electronic Blackmail Methods against Children on the Dark Web and Their Psychological Impact 197
Noha Abd El Salam Abd El Tawab Soliman Kedwany

Combating Child Sexual Exploitation on the Dark Web: Technical, Legal, and Psychological Perspectives 223
Ramy El-Kady

"Artificial Intelligence and Digital Sexual Exploitation of Children on the Dark Web: A Study of Challenges and Mechanisms" 263
Sameh El-Saeed

From Manipulated Word to Manipulated Algorithm 291
Katarina Smakic, Nenad Putnik, and Milica Boskovic

Contributors

Mohammad Elhady Abdelhakiem Ratib Abdelhafiz Dubai Police Academy, Dubai, UAE;
Faculty of Law, Assiut University, Assiut, Egypt

Ahmad Alsuwaidi Dubai Police Academy, Dubai, UAE;
Nicosia University, Nicosia, Cyprus

Ibtesam Mohamed Al Awadhi Dubai Police Academy UAE, Dubai, UAE

Hesham Badawy IEEE EGYPT Section, Alexandria, Egypt

Milica Boskovic Faculty of Diplomacy and Security, Belgrade, Serbia

Irenee Dondjio Nicosia University, Nicosia, Cyprus

Amar Yasser El-Bably Egyptian Police Academy, Cairo, Egypt

Ramy El-Kady Dubai Police Academy, Dubai, United Arab Emirates

Sameh El-Saeed Assistant Professor at Police Science Department-Criminal Justice College-Naif Arab University for Security Sciences, University in Riyad, Riyad, Saudi Arabia

Hossam Nabil El Shenraky Head of Police Management Department, Dubai Police Academy, Dubai, United Arab Emirates

Amer Fakhoury American University in the Emirates, Dubai, United Arab Emirates

Noha Abd El Salam Abd El Tawab Soliman Kedwany Waei Plus, Cairo, Egypt

Nenad Putnik Faculty of Security Studies, University of Belgrade, Belgrade, Serbia

Eldar Saljic American University in the Emirates, Dubai, UAE

Katarina Smakic Faculty of Diplomacy and Security, Belgrade, Serbia

Dusko Tomic American University in the Emirates, Dubai, UAE

Investigating Deepfake AI-Generation of CSAM and CSEM (Challenges and Solutions)

Hossam Nabil El Shenraky

1 Introduction

The rise of AI-generated child sexual abuse material (AIG-CSAM) has emerged as a significant concern in the field of child protection, posing unique legal and ethical challenges. With AI tools such as generative adversarial networks (GANs) and autoencoders becoming increasingly accessible, offenders have harnessed these technologies to create highly realistic depictions of child sexual exploitation. Unlike traditional forms of CSAM, which involve real victims, AIG-CSAM is often synthetic, generated from images or data sets without the direct involvement of actual children. Despite this, the psychological and social harm caused by such materials remains profound, as offenders use these images to fuel sexual exploitation, desensitize communities, and, in some cases, engage in extortion and grooming.

The proliferation of AIG-CSAM is largely enabled by the availability of open-source AI platforms, which allow users to generate synthetic media with minimal oversight. These tools, often developed for legitimate purposes, are being repurposed to create explicit content involving children, leading to a disturbing trend where offenders increasingly refer to themselves as "artists" within dark web forums. Moreover, this growing trend has captured the attention of stakeholders in education, law enforcement, and the tech industry, prompting urgent discussions about how to combat this new form of exploitation. The 2023 report from the Internet Watch Foundation (IWF) highlighted the unprecedented scale of CSAM incidents, driven in part by the misuse of AI technologies.

This chapter aims to explore the mechanisms behind AIG-CSAM creation, its impact on children, and the current regulatory and technological gaps. By examining

H. N. El Shenraky (✉)
Head of Police Management Department, Dubai Police Academy, Dubai, United Arab Emirates
e-mail: habdelraouf@dubaipolice.ac.ae

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_1

the ethical ramifications of AI-generated content, the chapter will also propose strategies for mitigating the spread of AIG-CSAM and safeguarding vulnerable populations. The evolving nature of this issue demands swift action, with a focus on collaborative efforts between technology developers, policymakers, and child protection advocates to prevent further harm.

2 Keywords

AI developer, AI-generated child sexual abuse material (AIG-CSAM), AI provider, Adult sexual content, Broadly shared models, Child safety policy, Child sexual abuse material (CSAM), Child sexual exploitation material (CSEM), CSAM advertising, CSAM solicitation, Data hosting platform, De-aging, Fine-tuning, Grooming.

3 Aims and Objectives

2.1 Understand AI-Enabled Exploitation Techniques
2.2 Highlight Policy Gaps
2.3 Evaluate the Ethical Ramificationsn
2.4 Propose Technological Safeguards and Policy Solutions

4 Method

The current study reviewed previously published quantitative studies focused on the technological behaviors of online CSEM offenders. This review covered a range of sources, including peer-reviewed journal articles, conference proceedings, and gray literature such as graduate theses, government reports, and industry publications. Studies that lacked significant quantitative data but offered relevant theoretical insights or summaries were used as background references. These sources were cited in appropriate sections to provide context, though they were not included in the main quantitative analysis. This approach ensured the analysis remained focused on measurable behaviors, while also drawing on broader insights to support and contextualize the findings.

5 Literature Review

5.1 The Technology Behind Deepfakes

Deepfake technology is a rapidly evolving branch of artificial intelligence that has transformed the landscape of media creation, with applications ranging from entertainment and art to disinformation and non-consensual content. The underlying methods used to create deepfakes involve advanced machine learning models, specifically Generative Adversarial Networks (GANs) and autoencoders (Goodfellow et al., 2014).

GANs, developed in 2014, are the primary drivers of deepfake technology. They consist of two neural networks: a generator and a discriminator, which work together in a competitive loop. The generator creates synthetic data, such as images or audio clips, that mimic real data, while the discriminator works to distinguish between authentic and generated content (Schwartz, 2018).

This process results in highly realistic synthetic media that can appear strikingly similar to actual photos, videos, or audio recordings. When trained on face images, for example, GANs can produce realistic faces by learning from the dataset's characteristics without replicating any single face directly (Andrews, 2019).

Reconstructs the face of Person B with the expressions and orientation of Face A. To produce a convincing video, this has to be done on every frame.

With applications like face-swapping, whole-body transformations, or synthetic voice creation, GANs have enabled the creation of increasingly accurate and believable media. As shown in Fig. 1, Autoencoders, another technique employed in deepfake creation, are composed of an encoder, which compresses an image by distilling its essential features, and a decoder, which reconstructs the image from those features. In a deepfake context, two autoencoders work in tandem with a shared encoder but separate decoders.

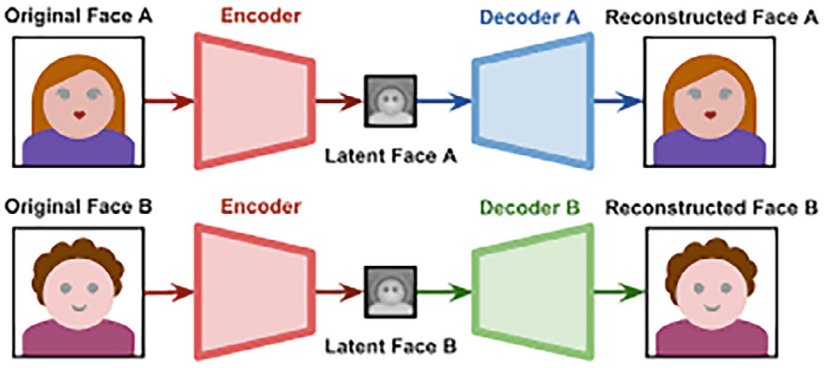


Fig. 1 The structure of autoencoders used in deepfake creation, illustrating the encoder for feature extraction and decoders for image reconstruction, enabling accurate and believable transformations

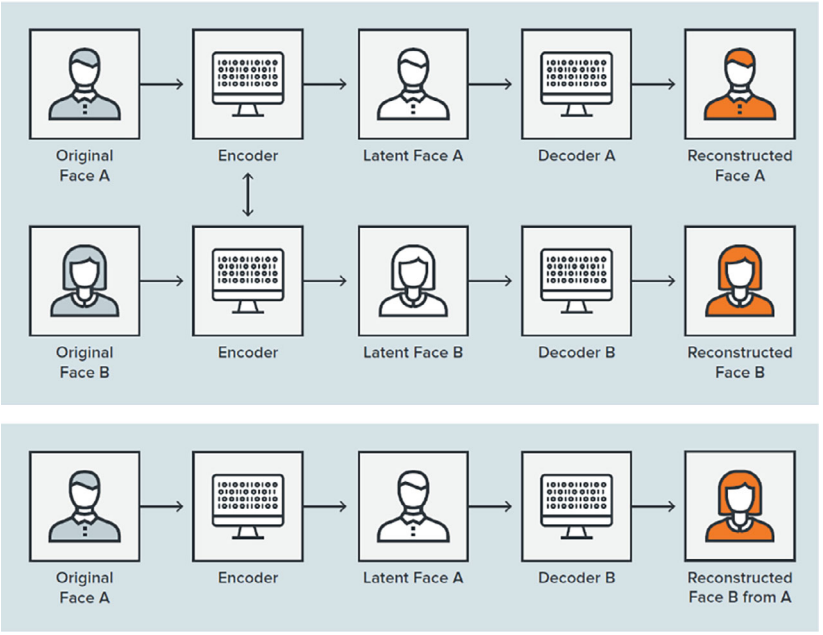


Fig. 2 A deepfake creation model using two encoder-decoder pairs. Two networks use the same encoder but different decoders for the training process (top). An image of Face A is encoded with the common encoder and decoded with Decoder B to create a deepfake (bottom)

This setup allows the encoder to capture commonalities between two faces—such as the positioning of eyes, nose, and mouth—while the decoders reconstruct each face individually. As Fig. 2 (https://www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf).

illustrates, this process enables face-swapping, where the expressions of one person (Face A) are transferred onto another (Face B), creating the illusion that Person B's face is expressing Person A's features and expressions. To maintain consistency, this manipulation is applied frame-by-frame in a video, resulting in a seamless transformation (Samantha, 2020).

Another facet of deepfake technology involves speech synthesis, which uses machine learning models trained on an individual's speech patterns to generate synthetic audio, often called "voice clones." By gathering data from public recordings—such as interviews, conference speeches, or social media videos—these models replicate vocal patterns, including tone, accent, and inflection, to create "voice skins" that sound convincingly like the original speaker. This technology has been used to both beneficial and malicious ends, as realistic voice clones enable applications in entertainment, accessibility, and impersonation (Patrini, 2019).

Deepfakes can take many forms, including face replacement (swapping one face for another in a video), face re-enactment (manipulating lip movements or expressions), and face generation (creating entirely fictional faces). Shallow fakes, while

not technically deepfakes, also contribute to the spread of disinformation. These simpler manipulations involve basic editing, like slowing down footage or altering the video context, to create misleading impressions. Shallow fakes are generally less sophisticated than AI-generated deepfakes, but they can still distort reality and alter public perception, making them part of the broader deepfake phenomenon (Criminal Misuse of AI and Deepfakes, 2020).

Despite the potential for misuse, the adoption of deepfake technology among criminals remains limited. Several factors contribute to this, including the brief impact lifespan of fake content, the high technical skill required to produce believable deepfakes, and the reliance on established criminal techniques that are often simpler and more cost-effective. Although the tools to create deepfakes are widely available, the time and expertise required to produce high-quality results make them less attractive for many criminals, especially compared to traditional methods of deception or fraud (Levine, 2014).

In response to the rise of deepfake media, significant effort has been invested in developing detection techniques. AI-driven tools are a key part of this effort, with algorithms designed to identify patterns and inconsistencies that indicate manipulation. For example, tools like Face Forensics++ analyze features such as lighting inconsistencies, lip synchronization issues, and unnatural facial expressions. These tools have shown high success rates in identifying deepfakes, surpassing the accuracy of manual inspection, which can be limited by psychological tendencies to believe audio-visual content as real (Rössler et al., 2019).

Blockchain technology offers an additional verification layer by authenticating the origin of media files, potentially limiting the spread of unverified content. Blockchain-based tools that label videos as "verified" can help identify trusted sources, ensuring that only legitimate content is disseminated. Another promising approach involves spectrogram analysis, particularly for deepfake audio detection. Spectrograms—visual representations of audio clips—reveal unique patterns in genuine versus synthesized audio, enabling AI algorithms to differentiate real speech from manipulated content (Yuezun Li et al., 2018).

Many organizations are investing in research and development to improve deepfake detection. In recent years, major tech companies and international organizations have collaborated to advance detection technologies (Manke, 2019).

For example, Microsoft, Facebook, and Amazon launched a Deepfake Detection Challenge to encourage innovation in this area, with Microsoft later releasing the Video Authenticator tool, which provides users with a confidence score indicating whether a video has likely been manipulated. Furthermore, Facebook released an open-source dataset of 100,000 deepfakes to train detection models, recognizing that such publicly available data is essential for building effective AI-enabled detection tools (Martínez, 2018).

As deepfake technology becomes more sophisticated and accessible, detection will increasingly rely on a combination of advanced AI, cross-industry collaboration, and public awareness. Detection tools must continuously adapt to advancements in synthetic media, as deepfake techniques become more refined and capable of bypassing current detection methods (Brenner, 2019).

Public–private partnerships, investments in open-source data, and ongoing research will be critical to developing scalable solutions capable of protecting digital media integrity in the face of rapidly evolving (Detecting Audio Deep Fakes With AI, 2019).

Furthermore, the social media industry can also play a key role in improving deepfake detection by providing publicly available data to properly train AI-enabled detection tools. For instance, Facebook has released an open-source database of 100,000 deepfakes to train AI models to spot manipulated videos (Will Douglas Heaven, 2020).

As the degree of sophistication for generating deepfake technology continues to improve, it will ultimately take a combination of techniques to enable the detection of synthetic or fake videos and images (Vincenzo Ciancaglini et al., 2020).

5.2 The Challenges of the CSAM and CSEM Investigation in the Dark Web

It requires a series of peer-to-peer networks that are not able to access by regular ways and are not indexed by traditional browsers (Olson, 2022).

Dark Web is accessible via a specific browser which is onion, so users can use it to browse hidden and illegal websites, it can be considered hosted within vpn which add challenges to trace locations of the hosting server cannot which consider high challenge of the investigation in cybercrime, while it is anonymous totally, it encourages criminal groups to use it in connecting each other and to commit their criminal activities (Ofusori & Hendradi, 2023, Kaur & Randhawa, 2020, IWF, 2021, Spalevic & Ilic, 2017).

Anonymity allowed criminals to use it for illegal purposes, The growth of black markets gave chances for illegal activities to be committed and enhanced the capabilities of criminals to commit their crimes with anonymity (Shakarian, 2018).

One of the most important chances for those criminals is that they could use it to enhance children's sexual exploitation. that it gave them capabilities to share CSAM depicting rape and sexual abuse images and videos of children, from all over the world without being traced (*Deepfake Detection Challenge Dataset,* 2020).

We can notice a new methods of child sexual exploitation with the evolution of using GAI in children photos and videos creation that are sophisticated, publicly accessible and, in many instances, offenders who seek to exploit children are once again among the earliest adopters of GAI platforms and are challenging existing protocols and legal remedies available to protect child victims by manipulating GAI tools and employing them to exploit children in varied and escalating manners (Mehta, 2020).

5.3 Users Seeking to Alter Known CSAM Imagery to Create New CSAM Imagery Using Gen-AI Platforms

- In January 2024, law enforcement submitted CSAM seized from an offender to NCMEC's Child Victim Identification Program. Upon review of the imagery, NCMEC determined that the content consisted of known CSAM images depicting multiple victims who had been identified and recovered in 2007 and 2018. The known CSAM images had been altered using GAI technology to add faces of unknown children to the imagery, while retaining the sexually abusive components of the known images.
- NCMEC's Cyber Tipline has received reports from GAI platforms relating to users uploading/attempting to upload known CSAM imagery to be used to create new CSAM imagery.

Altering innocuous images of a child to generate sexually explicit/abusive images:

- NCMEC has received multiple reports from members of the public relating to at least three separate instances in which minor boys have used "nidify" or "unclothe" GAI platforms to create nude/sexually exploitative images of their female classmates based on innocuous images shared on social media. Many of these cases involved the creation of hundreds of images depicting multiple female victims that were shared on social media.
- NCMEC's Cyber Tipline has received reports from GAI platforms relating to adult users uploading innocuous images of minors and attempting to use GAI platforms to sexualize the images.

One recent report involved a user who was identified as a doctor with possible direct access to minors.

"SCARY real and there's even a video of me doing disgusting things that also look SCARY real. I don't know how the person managed to make them look that real. I did end up sending …my debit card information…."

Offenders also are actively collaborating on dark web sites to share GAI CSAM imagery and to exchange suggestions for how to use GAI platforms to generate CSAM imagery.

- "AI generative CSAM as a CRIME? its 100 percent Victimless!! It's about anyone who has this attraction and your it is not a choice, but it's about jailing us. They believe they can slowly get rid of all the pedophiles, but they won't or can't."

While CSAM and child sexual exploitation content can be created on Gen-AI platforms, this content is frequently shared on traditional online platforms, including mainstream social media platforms.

V. Impact of GAI Technology on Child Safety and Potential Solutions to Better Protect Child Victims GAI technology has been widely available to the general public for just over a year, yet already has raised significant concerns and impacted child safety. Against this rapidly evolving landscape, NCMEC has identified several

operational and legal concerns, as well as potential areas to develop best practices, new legislative/regulatory measures, and strengthen legal protections for victims, including the following items:

A. Areas of Concern Relating to Impact of GAI Technology on Child Safety Rising Volume of CSAM and Sexually Exploitative Imagery of Children—the volume of GAI CSAM and sexually exploitative content reported to NCMEC in 2023 (4,700 reports) is minor compared to the more than 36 million.

Cyber Tipline reports NCMEC received last year. However, as GAI technology becomes more accessible, capable of producing sophisticated image—and increasingly video—content, and continues to exist in open-source forms without training parameters for the underlying machine learning technology, NCMEC is concerned that GAI CSAM reports will lead to even more dramatic increases in reports. This has the potential to strain NCMEC and law enforcement resources, in addition to further normalizing the sexual exploitation of children within society.

Potential Legal Uncertainty Relating to Criminal and Civil Remedies for Children Victimized by GAI Imagery—currently there is some uncertainty regarding precisely how existing criminal and civil laws at the federal and state levels will apply to protect children victimized by GAI CSAM and sexually exploitative/nude images. As more legal cases involving GAI imagery move forward, certain gaps and essential refinements in the law likely will be highlighted that will require legislative action.

Difficulty Distinguishing a "Real" Child from a Child Depicted in GAI CSAM—there are concerns that the proliferation of GAI CSAM images will complicate child identification efforts undertaken by NCMEC and law enforcement. In conducting victim identification of children depicted in CSAM imagery, it is essential to be able to determine if the child victim is a real child and if the offender has access to that child in real life. GAI CSAM complicates child victim identification because now NCMEC and/or law enforcement first must determine which cases depict a real child in need of rescue and which child victims are GAI generated for an offender's personal gratification. An additional concern is that offenders will produce CSAM with a real child victim and then use GAI technology to alter the imagery in order to avoid detection or identification of the victim.

GAI Technology Accelerates Enticement/Sextortion—the use of GAI technology to accelerate enticing and sextorting (including through financial sextortion), a child is an especially troubling trend. An offender previously had to manipulate or trick a child into sharing a nude or sexually exploitative image of themselves prior to sextorting them. With GAI technology, an offender only has to locate innocuous images of a child on social media, sexualize the images using a GAI platform, and then can sextort the child for additional imagery or, more often, financial payment upon a threat that the offender will circulate the GAI imagery to the child's friends and family members online.

New Victimization for Identified/Recovered Survivors—the use of GAI platforms to create new CSAM imagery based on existing, known CSAM imagery is especially insidious. Survivors already grapple with the knowledge that imagery depicting their abuse as children continues to circulate online long after their recovery and as they enter adulthood. Sexually explicit and abusive images in which these survivors are

depicted can now be altered and expanded in number by using GAI technology. Additionally, non-explicit images can be altered to create new explicit content contributing to further victimization and harm. The cycle of trauma for these survivors now continues in new ways, with feelings of loss of control, lack of trust in technology, and exposure complicating a victim's recovery process. No matter how CSAM, sexually exploitative, or nude imagery is created:

directly by offenders, through enticement or manipulation and threats to the victim, or through GAI, the impact on the child is real and devastating (Testimony of John Shehan, 2024).

5.4 Unveiling the Challenges of AI-Generated CSAM

The impact of using AI-generated to generate CSAM is significant, and it is considered a challenge, so in case of real child's likeness is used, the photos can be harmful to the physiology of the victim, and support the desensitization of offenders.

CSAM as generated by AI or not consider as useful tool for investigators, but it can't remove the harm that happened in generating and spreading those photos.

While the development of innovative AI detection tech. is crucial, it is important to prevent the issuing and sharing of child exploitation content.

The other challenge is the open-source nature of many generative children's sexual photos and videos tools, which are privately accessible and lack moderation, it is hard to prevent offenders from using them to harm or to monitor their usage.

There is a misconception that removing CSAM from AI training datasets will eliminate the dilemma of AI-generated CSAM, it is not straightforward, because it is able to compile many concepts learned during training.

For example, they can compile concepts learned from CSAM photos of children with concepts from photos with adult sexual content, which means that if CSAM is removed from the training data, generative AI models it could generate AI- CSAM or other materials, considering other sexual exploitation photos contained in AI training datasets.

Also, with open-source generative models like Stable Diffusion, anyone can fine-tune it on their datasets, making them capable of generating certain types of CSAM photos.

While it might be removed from AI training sets, the issue of AI-generated CSAM is more complex than just filtering out certain photos from training data.

IWF report mentioned that AI-generated CSAM are enhancing their realistic, videos are likely to improve, and open-source tools to generate it will be more accessible. We are also hearing about more finetuned models created for a real child's identity, which allow perpetrators to invent different types of pictures of any child (Dr Shaunagh Downing, 2024).

5.5 AI-Produced Child Sexual Abuse Material: Insights from Dark Web Forum Discussions

IWF's 2023 report found that offenders are taking snapshots of children, often popular children, and using ML models to generate AI CSAM, there are major categories of AI CSAM recently:

(1) AI-manipulated CSAM, where photos and movies of real children are altered into sexually explicit content.
(2) AI-generated CSAM in which entirely new sexual photos of children are manufactured (Krishna et al., 2024).

Researchers at the International Policing and Public Protection Research Institute (IPPPRI) wanted to understand more about what Dark Web forum members were saying and doing with regard to AI CSAM. To do this we decided to examine Dark Web forum members' posts and discussions about AI CSAM. Researchers collected conversations through Voyager by (OSINT) platform that collects, stores and structures content from publicly accessible open sources including Dark Web forums where CSAM related discussions took place.

The Web-IQ issued a Hash Check Server (HCS). (see Fig. 1), E-service providers use it to detect whether images or videos stored on their platform constitute known CSAM. It also enables them to block known CSAM before it is re-uploaded. The service is available to service providers worldwide. Billions of images have already been checked, and millions of images and videos have been blocked from being watched by other users.

The HCS can scan shared photos spreading on the darknet, which provides specific insight into CSAM spreading.

As shown in Fig. 2, online offender communication is retrieved through the dark web and made available to LEA via the Voyager Intelligence app. also the Languages used, locations mentioned and relationships between users will support authorities challenges, these discussions enhance the security and awareness of using the internet by criminal techniques about threats that children face online.

5.6 ICTs and AI-Generated CSAM

Using ICTs can change the methods of generating and spreading child sexual content, The ability to generate child sexual exploitation content enhanced as E- images can be generated cheaply without the need for external processing and generate with high quality, Cyberspace enabling opportunity to spread sexual content of children in large volumes, with minimal cost and relative anonymity (Clough, 2010, p. 249).

5.7 Virtual Child Pornography

As the production, possession, and distribution of child pornography are a serious offense in most countries, the perpetrators always try out new ways so that their activity falls into a gray zone of legality,

which lowers the likelihood of persecution. It is much easier now, as technology has advanced to the point where a realistic depiction of a child can be created without a real child being involved (Gillespie, 2010, p. 211).

The term "virtual child pornography" in a wider sense refers to child pornography in cyberspace (including those with real children involved) while in a narrower, and more commonly used, sense it is pornography directly linked to cyberspace as it can only be produced in cyberspace (Poborilova, 2011, p. 242).

There are three principal ways of creating virtual child pornography:

(1) manipulating existing images (pseudo-photography)
(2) computer-generating new images 3) dressing up adults as if they were minors (Gillespie, 2010, pp. 211–212).

Some authors use "pseudo-photography" and virtual child pornography interchangeably (Gillespie, 2016, p. 245) but the latter term is wider and can include other forms of media like cartoons, manga, anime, etc. Pseudo-photography is created by digitally altering images, "blending" or "morphing" several together, for example putting a child's face on an adult's body to make it appear as if it is a child who is engaged in sexual activities (Greijer & Doek, 2016, p. 41).

The main distinction is that some photos are only computer-manipulated while others are computer-created. Manipulating photos can result in a new photograph that never actually took place, even videos can be easily manipulated by the use of Deepfake, a technique for human image synthesis based on artificial intelligence, creating false images in only a few hours (Gillespie, 2016, 245–246, Harris, 2019, p. 100).

This can be utilized to produce child pornography and can be considered virtual child pornography.

Computer-created photos are fully generated by a computer and are not derivatives of photographs, it must be noted that despite the rapid development of technology it appears that for the foreseeable future child pornography is likely to be created using real children (Clough, 2010, p. 272).

5.8 *How AI is Being Abused to Create Child Sexual Abuse Imagery*

5.8.1 Image Generation

As shown in Fig. 3, the advancement of AI-generated sexual content has accelerated with the introduction of sophisticated applications such as Midjourney V4. This version significantly enhances the quality of generated content, with subsequent releases like V6.1 offering improvements in image coherence, resolution, detail accuracy, and overall text quality. New features include better personalization and texture enhancement, demonstrating the rapid evolution of AI image generation technologies.

Among the notable advancements is Stable Diffusion XL (SDXL), which provides photorealistic outputs with detailed imagery and improved face generation capabilities. Released in September 2023, DALL-E 3 has also garnered attention for its impressive image generation abilities, showcasing the competitive landscape of AI tools. These leading models primarily rely on diffusion techniques, which involve adding random noise to images and then systematically removing it to create new visuals. They are trained on extensive datasets, such as the LAION dataset, which comprises millions of labeled images sourced from the internet.

Despite the advancements, the proliferation of high-quality AI-generated images raises ethical concerns, particularly regarding their potential misuse for creating non-consensual content. Ongoing discussions emphasize the importance of establishing digital watermarking measures to enhance the identification and admissibility of AI-generated media while mitigating risks of manipulation. Technologies like Google's Synth ID, which embeds watermarks at the pixel level, represent steps toward addressing these concerns, although challenges remain in developing reliable detection tools due to the possibility of metadata alterations.

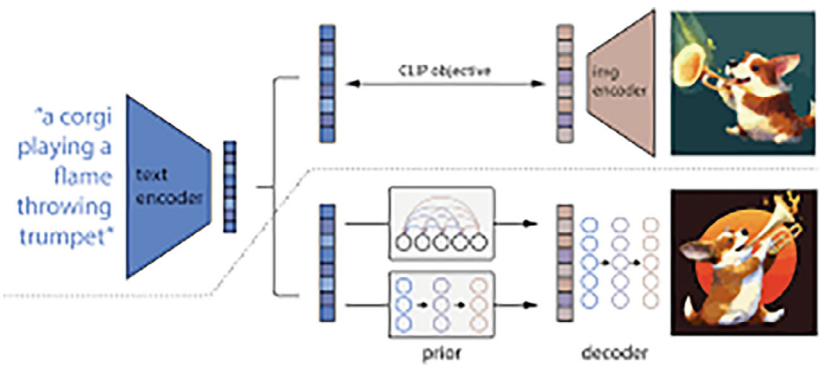


Fig. 3 Demonstration of AI advancements in image generation, showcasing how text inputs are transformed into detailed and coherent visuals using enhanced encoder-decoder architectures

5.8.2 Factors Influencing the Spread of CSAM

The concept of AI-generated CSAM is not new, this type of material became more dangerous, by the appearance of the deepfakes (*What is Deepfake Technology and How Are Threat Actors Using It?*, 2023).

Deepfakes technology facilitated the possibility of generate children sexual materials through GEN- AI that the child in a video appears to be another child, it uses face swapping and puppeteering to maliciously to spread wrong data.

(Gen- AI) taking this sexual exploitation for children to a dangerous level, especially that this technology spread and developed very fast and its tools became available, with no consideration given to what guardrails might be needed (Jaiman, 2022).

The investigations about the GenAI CSAM increased regarding real-life abuse children, offenders by this technology can replace a child's character with another child who has not been sexually abused, and when authorities investigate that exploitation against that child whey will not be able to detect victim.

The capability of replacing a child's character using Gen-AI can endanger the child who was not exploited through sextortion tools based on the "fictitious" image (David Thiel et al., 2023).

Though researchers found that not more than 1% of CSAM found in known offenders' environment was GenAI image realistic which could dire negative effects on the CSAM (Lapowsky, 2023).

While some Gen-AI producers put measures to prevent the generation of CSAM using AI, open-source websites were much slower to comply with such precautions, these websites enabled production of GenAI CSAM But it facilitated the generating of CSAM, using photos of real children as source material (Verma & Oremus, 2023).

The impact of generative AI on CSAM based on it is harnessing and regulating, the harms and impact of GenAI CSAM are significant, and photo-based sexual exploitation of a child whose picture used to generate CSAM, the revictimization of children by producing progressively exploit AI-generated versions of abuse, the potential for the material triggering an interest in CSAM that escalates to contact offending, all potential issues. The images might be "fake," but dangers and abuse are real.

Fields of concern of police agencies concern that are mandated to identify and appropriately code AI produced CSAM and apprehend offenders.

1. Forum members learning using technology to generate AI CSAM or manipulated photos.
2. Members of forums are sourcing photos of children from other members to manipulate it.
3. Members of forum move from the generating "softcore" AI-CSAM to "hardcore" material.
4. Members of forum extensively sharing AI- generated CSAM, and encouraging users on Dark Web sites to generates and exchange their images and videos, and contributing to escalation and expansion of offending in CSAM crimes (Davy & Lundrigan, 2024)

The October 2023 report emphasized significant issues surrounding user-friendly online AI pornography services, specifically focusing on the creation of fully synthetic sexual content involving children. Although there remain obstacles for users attempting to generate images with AI text-to-image models—such as the necessity for specific technical skills and appropriate computer hardware—some platforms have been developed to make the process more accessible. These services facilitate the quick and intuitive creation of child sexual abuse material (CSAM), allowing users to simply input their preferences without needing to download or install applications.

Additionally, the report noted that there is evidence of offenders who have tried and failed to create AI-generated CSAM using these platforms, with instances documented in prior IWF reports. Nevertheless, between April 2023 and March 2024, there were two significant reports that indicated offenders successfully generated AI CSAM using these services. This underscores a concerning reality in which such platforms enable the production of harmful content, despite ongoing efforts to control and address their influence.

Notably, As demonstrated in Fig. 4 (What has changed in the AI CSAM landscape, *IWF,2024*, p:22. https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf), the proportion of Category A images has increased by 10 percentage points. This could indicate that technology and expertise has advanced such that perpetrators are experiencing more success generating "hardcore" scenarios—generally, penetrative sexual activities—complex scenes involving multiple individuals, which image-generating AI has historically had greater difficulties producing accurately compared to scenes involving just one individual, Just as in the previous snapshot, shown in Fig. 5 (What has changed in the AI CSAM landscape, *IWF,2024*, p:10. https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf), female children featured in over 99% of AI CSAM images assessed (What has changed in the AI CSAM landscape?, 2024).

5.9 AI Tools Used to Generate Fully Synthetic Videos

Recent developments have led to notable advancements in the creation of fully synthetic realistic video content, highlighted by the introduction of several new video generation models: Stable Video Diffusion (released in November 2023), Sora (previewed in February 2024), and Veo (previewed in May 2024). OpenAI's Sora can generate realistic minute-long videos from scripts, photos, or existing video footage, and has been shared with select researchers, with plans for a public rollout in the near future.

Both Sora and Veo are positioned at the forefront of the video generation industry, utilizing a research-only preview approach prior to their full public releases. In contrast, Stable Video Diffusion offers the ability to create short videos from images

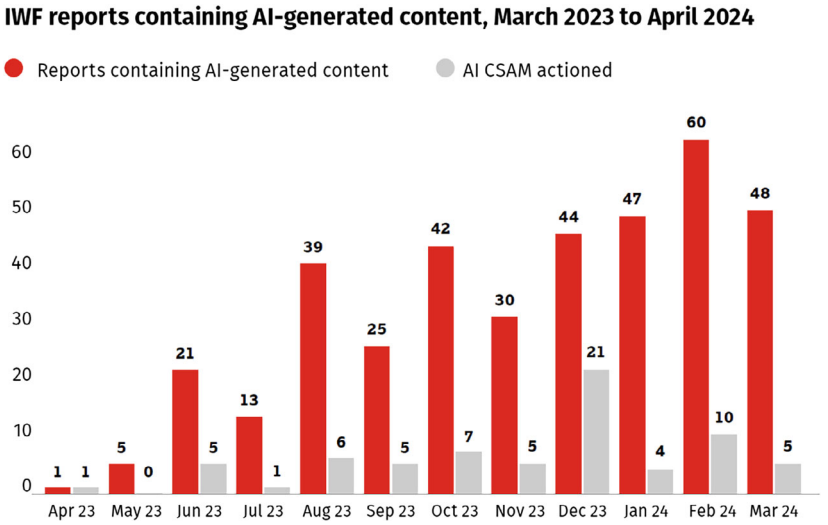


Fig. 4 Monthly IWF reports on AI-generated content from March 2023 to April 2024, highlighting the increase in reports (red) and the corresponding AI CSAM cases actioned (gray)

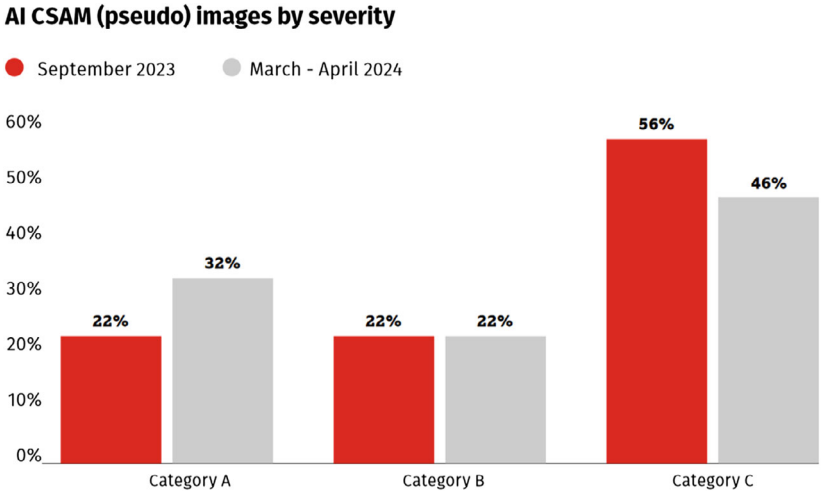


Fig. 5 Distribution of AI-generated CSAM (pseudo) images by severity categories, comparing percentages from September 2023 (red) with March–April 2024 (gray)

and is available as an open-source model under a non-commercial license. Its functionality is similar to that of the closed-source Runway ML Generative model, underscoring the competitive nature of the AI video generation landscape (*OHCHR | Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment*, 2024).

5.10 Livestreamed Child Sexual Abuse

Livestreaming of child sexual abuse material (CSAM) has emerged as a concerning reality, allowing perpetrators to broadcast live abuse over the internet using webcams. This enables offending viewers to witness the acts in real time, with such material being shared on various platforms, including chatrooms, social media, and increasingly popular video conferencing applications. In many instances, the sexual acts are directed by the viewers themselves.

When the livestream concludes, evidence of the abuse may vanish unless the offender has deliberately recorded it, resulting in a lack of digital trace that makes it challenging for law enforcement to gage the scope of the issue and take appropriate action. Furthermore, software can be employed to produce permanent recordings of the livestreamed abuse, facilitating the later distribution of these captured images. This type of abuse is often described as "distant livestreamed child sexual abuse," as much of the content is streamed across international borders, complicating efforts to combat it effectively (*A Report About Child Sexual Abuse Crime*, 2019).

6 Case Study Analysis

In May 2024, Steven Anderegg, a 42-year-old man from Holmen, Wisconsin, became the subject of the first federal charge in the U.S. involving entirely AI-generated child sexual abuse material (CSAM). Federal prosecutors allege that he used the popular AI image generator Stable Diffusion to create over 13,000 explicit images of minors, many of which depicted fully or partially nude children engaging in sexual acts. A Justice Department official stated that this case marks a significant legal precedent, as it is believed to be the first instance where someone has been charged for using AI to fully generate CSAM. Notably, the images created did not feature real children but were produced by inputting text prompts into the AI generator. This aligns with arguments from Justice officials that existing laws banning photorealistic fake and obscene images, established in 2003, apply to AI-generated content.

In addition to Anderegg's case, two recent investigations in North Carolina and Pennsylvania revealed that men had used AI to create deepfake images, superimposing children's faces onto explicit scenes or digitally altering photographs to remove clothing from minors. These developments have raised alarm among child safety researchers, who noted that such tools are being promoted on pedophile forums to create highly realistic and uncensored depictions of children. The case highlights a relatively untested legal pathway that federal officials intend to explore, asserting that AI-generated images should be treated similarly to real-world child sex abuse material (Mahmud & Sharmin, 2023).

Ella Irwin, a senior executive at Stability AI, which developed Stable Diffusion, stated that the materials in question were produced using an earlier version of their software. Despite implementing safeguards, including filters to block unsafe prompts,

Stability AI acknowledged that open-source versions of the software exist, allowing users to bypass these filters. Federal officials have expressed concerns that while they aim to enhance the difficulty for offenders to misuse future AI tools, savvy individuals can still exploit earlier versions without detection.

In September 2023, Anderegg shared an Instagram story featuring a realistic AI-generated image of minors in bondage-themed clothing, inviting viewers to join him on the messaging app Telegram. He also allegedly communicated with a 15-year-old boy on Instagram about his methods for generating explicit images, sharing multiple AI-created images of children. This activity prompted Meta, Instagram's parent company, to report his account to the National Centre for Missing and Exploited Children (NCMEC), which subsequently provided "Cyber Tip" reports to Wisconsin law enforcement (Valle, 2024).

Law enforcement executed a search warrant at Anderegg's home in February 2024, where they discovered that he was familiar with Stable Diffusion and had installed the software alongside add-ons for generating explicit content. Evidence suggested he had used extremely specific prompts to create the troubling images. Initially charged with state offenses such as "exposing a child to harmful material," Anderegg later faced federal charges under the Protect Act of 2003, which prohibits the creation of computer-generated imagery depicting minors in sexually explicit conduct (Bureau, 2024).

This case, along with others like it, underscores the growing crisis in child pornography fueled by AI image generators. As the technology evolves, it becomes increasingly capable of producing hyper-realistic child exploitation images, posing challenges for law enforcement and child safety experts. A study by Stanford University's Internet Observatory revealed a significant number of photos of child exploitation in open-source databases that AI models rely on. Legal experts have noted the importance of leveraging existing laws to address the challenges posed by AI-generated CSAM, emphasizing the need for urgent action to protect vulnerable populations (*Charlotte Child Pornography Case Shows 'Unsettling' Reach of AI Imagery*, 2024).

CHARLOTTE, N.C.—David Tatum, 41, a child psychiatrist in Charlotte, was sentenced to 40 years in prison followed by 30 years of supervised release for sexual exploitation of a minor and using artificial intelligence (AI) to create child pornography images of minors, announced Dena J. King, U.S. Attorney for the Western District of North Carolina.

Tatum was also ordered to pay restitution in an amount to be determined within 90 days, a $100 special assessment per count of conviction, and a special assessment totaling $99,000 under the Amy, Vicky, and Andy Child Pornography Victim Assistance Act (AVAA). After he is released from prison, Tatum will also be required to register with the Sex Offender Registry Board in any state or jurisdiction where he works or resides (*Western District of North Carolina | Charlotte Child Psychiatrist Is Sentenced To 40 Years in Prison for Sexual Exploitation of A Minor And Using Artificial Intelligence to Create Child Pornography Images Of Minors | United States Department of Justice*, 2023).

This case underscores a troubling evolution in criminal methods involving CSAM, revealing how AI advancements are enabling new forms of exploitation that challenge

existing prevention, detection, and legal frameworks. Here are some key conclusions about the development of criminal methods in CSAM:

Shift from Real-World Exploitation to Synthetic Creation: the ability to generate photorealistic CSAM entirely through AI marks a significant shift from methods that involve real-world exploitation. Previously, CSAM offenses relied on actual minors being victimized, but AI now allows offenders to create realistic depictions without involving real children directly. This shift not only lowers the risk of detection but also circumvents some current legal definitions, which were originally written to address crimes with real victims.

Despite this, such material still fuels demand, normalizes harmful behavior, and potentially encourages offenders to engage in real-world exploitation (Parti & Szabó, 2024).

Increased Accessibility and Autonomy in Offense Execution Open-source AI models like Stable Diffusion enable offenders to create CSAM on personal devices, bypassing cloud-based restrictions or filtering mechanisms. This accessibility allows offenders to operate with more autonomy, making it harder for authorities and AI companies to monitor and detect these activities. With the ability to run software offline, offenders are shielded from the scrutiny of centralized oversight mechanisms, such as server-based monitoring and filtering systems.

By decentralizing CSAM production, offenders can avoid detection and control their entire process, posing a greater challenge to law enforcement's ability to prevent and track such activities.

Anonymity and Scalability: AI tools allow offenders to quickly generate vast amounts of content anonymously and in large quantities, as seen in the Anderegg case, where over 13,000 images were allegedly created. This scalability intensifies the potential harm, as offenders can create volumes of CSAM that would have required substantial time, risk, and access to real victims in the past.

The volume and ease of production also enable offenders to rapidly distribute large quantities of content through online platforms, messaging apps, and the dark web, further fueling demand.

Evolving Tactics in Concealing and Disseminating Content: the availability of open-source models allows for modifications that circumvent detection, with offenders customizing prompts and bypassing filters intended to block explicit content. For example, specific add-ons in Stable Diffusion were reportedly used by Anderegg to enhance the images for explicit purposes (Maddox & Apple, 2024).

Offenders are also increasingly using encrypted platforms and forums to share these AI-generated materials, making it harder for law enforcement to trace distribution channels or locate content creators.

New Legal and Ethical Challenges: the use of AI to create CSAM pushes the limits of existing legal frameworks, which were primarily designed to protect real children. Prosecutors are now applying the Protect Act to synthetic images, which could set a precedent for treating AI-generated CSAM as equally prosecutable. However, the evolving nature of these crimes means that further updates to laws may be necessary to clearly encompass AI-generated content and establish penalties that account for its unique characteristics (Downing, 2024).

This development prompts ethical questions about AI responsibility, with companies under increasing pressure to strengthen safeguards while balancing the benefits of open access and innovation.

Increased Pressure on Law Enforcement and Child Safety Organizations: with the rapid growth of AI-generated CSAM, organizations like the National Centre for Missing and Exploited Children face overwhelming volumes of content. Distinguishing between real and synthetic images requires advanced forensic tools, putting a strain on resources and complicating prioritization efforts, as real victims may be overshadowed by the influx of AI-based cases.

As AI tools continue to improve, child safety organizations and law enforcement agencies may need to invest in specialized technology and training to keep up with the sophistication of AI-generated content and enhance collaborative efforts with AI developers to minimize abuse.

The development of AI has significantly advanced criminal methods involving CSAM, enabling offenders to create and distribute realistic, synthetic images with unprecedented autonomy and scale. This shift requires an urgent response from lawmakers, AI companies, and child protection agencies to adapt regulations, enhance detection capabilities, and implement preventive measures in this new digital landscape. As criminal tactics evolve with technology, so too must the strategies and legal frameworks designed to safeguard vulnerable populations.

7 Findings

The growing misuse of AI technology to generate and manipulate images has sparked widespread public concern and prompted tighter legislative and regulatory measures, significantly shifting the risk landscape. AI-powered image generators, now widely accessible, have made it easier than ever to create and alter images, leading to a surge in activities involving child sexual abuse material (CSAM). Initially, adults engaging in these behaviors believed that generating and exchanging synthetic CSAM might not be illegal. However, with the rise of deepfakes and the widespread availability of social media platforms and mobile apps, the situation has worsened. Predators can now easily manipulate photos directly on their smartphones, often using images that children themselves have posted online. In some cases, these individuals take existing CSAM or child sexual exploitation material (CSEM) and superimpose the faces of children onto them. The availability of tools for generating manipulated content, coupled with the vast number of images children share on social platforms, has made it disturbingly easy for such images to be created and spread.

As deepfake technology becomes more widely used, what was once considered a speculative risk has become a far-reaching problem. In particular, schools have become the focal point of this growing concern, with significant media coverage highlighting incidents where students' images are being manipulated. This has led to an urgent debate among stakeholders about how schools can effectively discourage,

monitor, and respond to these emerging threats. The scale of the problem is underscored by 2023, which saw the highest number of reported CSAM incidents to date, as reported by the Internet Watch Foundation. Additionally, a global study on online abuse by the Child Light Global Child Safety Institute revealed alarming statistics in its "Into the Light Index." The study found that 1 in 8 children worldwide (12.6%) have been victims of non-consensual image offenses, and a similar percentage (12.5%) have faced online solicitation.

The rapid advancements in AI technology have played a significant role in enabling the creation of increasingly realistic CSAM images. Despite attempts by AI companies to introduce safeguards in their tools, these measures have proven inadequate. While newer versions of AI tools may include protections to make it more difficult to generate illicit content, many users can still access earlier or unregulated versions that lack such defenses. This ease of access to unprotected technology means that efforts to prevent the creation and dissemination of deepfake CSAM remain insufficient. As AI capabilities continue to improve, so too does the ability to create hyper-realistic, harmful content, making it clear that the issue of AI-generated CSAM is becoming more pervasive and harder to combat.

8 Discussion

The rapid emergence of AI-generated child sexual abuse material (AIG-CSAM) marks a pivotal and deeply concerning evolution in the landscape of child exploitation. This chapter's analysis highlights how offenders have quickly adapted to AI technology, using it to create synthetic yet realistic depictions of child abuse, often shared within dark web communities that encourage, refine, and normalize this behavior. The transition to AIG-CSAM not only amplifies the scale of abuse but also complicates its detection, making it a pressing issue for legal, ethical, and technical domains.

The open-source nature of many AI image-generation models, such as Stable Diffusion and Midjourney, poses a significant challenge for preventing AIG-CSAM creation. While these tools have legitimate applications, their accessibility and adaptability have allowed offenders to employ them in increasingly disturbing ways. The absence of rigorous safeguards or usage restrictions in these platforms enables bad actors to customize and fine-tune models, producing increasingly realistic and explicit material involving children. These tools' capacity for compositional generalization—combining different learned concepts to generate novel content—further complicates the issue, as they can merge images of children with adult content to produce disturbing outcomes even if training datasets omit explicit CSAM content. This calls for stricter controls, such as built-in watermarking and content provenance tracking, which could help detect synthetic imagery and prevent its spread.

AIG-CSAM inflicts real psychological harm, even in cases where the images do not depict actual children. Individuals whose likenesses are altered for these purposes experience violations of their privacy, identity, and sense of safety, leading

to profound emotional distress. The distribution of such content across dark web forums also fosters a subculture where child exploitation is normalized and even celebrated, further entrenching harmful attitudes toward children. Moreover, AIG-CSAM fuels demand within offending communities, perpetuating cycles of abuse and incentivizing the continued refinement of these images. As these communities grow, they pose a serious risk to societal health and well-being by fostering an environment where abuse is increasingly tolerated or downplayed.

AI developers and platforms play a crucial role in mitigating the misuse of their technologies. Integrating robust safety features into AI models, including adversarial misuse detection and automated monitoring, is vital in preventing these tools from being exploited to create AIG-CSAM. AI companies are ethically responsible for actively addressing the risks posed by their models, particularly as the technology becomes more advanced and available. Measures such as continuous stress-testing for model vulnerabilities and including feedback loops for ethical concerns are essential in creating a proactive approach to safeguarding against abuse.

A multi-faceted, coordinated approach is critical to address the rise of AIG-CSAM effectively. Lawmakers, technology developers, and law enforcement agencies must collaborate to bridge the gap between rapid technological advancements and the slower pace of legislative reform. Comprehensive legal frameworks are necessary to criminalize the creation, distribution, and possession of AIG-CSAM, ensuring that offenders face consequences even if no direct victim is involved. Technological measures, including AI-based detection tools, digital watermarking, and content tracking, are equally important in helping identify and control the spread of these materials. Additionally, public awareness campaigns and educational initiatives are essential in addressing the normalization of child exploitation within online communities and advocating for the responsible development and use of AI.

9 Conclusion

This chapter reveals the disturbing reality of AI-generated child sexual abuse material (AIG-CSAM) and the unique challenges it presents. With the advent of generative AI, offenders can now produce explicit images involving children without real victims, creating a morally and legally complex landscape. This development has transformed dark web forums, where offenders regard AIG-CSAM creators as "artists" and openly share techniques to refine and escalate the realism of their materials. The accessibility of open-source AI tools exacerbates this issue, as these technologies can be repurposed for illicit activities without adequate safeguards.

The rapid evolution of AI-driven CSAM production underscores the urgent need for coordinated action from governments, tech developers, and law enforcement. While traditional methods of combating child exploitation focused on tracking and removing real CSAM, AIG-CSAM adds layers of complexity, requiring new approaches to detection, regulation, and legal accountability. This chapter calls for robust technological safeguards, including digital watermarking, provenance

tracking, and rigorous stress-testing of AI systems to prevent misuse. Legal reforms must evolve to hold creators and distributors accountable, even when no real children are directly harmed.

In summary, AI has created new avenues for the exploitation of children's likenesses, raising critical ethical, technological, and legal questions. Tackling AIG-CSAM requires a proactive, multidisciplinary response that combines technological innovation with policy reform, ensuring that AI advances are safeguarded against abuse and that the rights and safety of children remain protected.

References

Andrews, J. (2019, Jul 12). *Fake news is real A.I. is going to make it much worse.* Retrieved Jun 26, 2020, from https://www.cnbc.com/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html

Bracket Foundation, UNICRI Centre for AI & Robotics, Clara Péron, Lisa Maddox, & Lana Apple, GEN-AI: A New Threat for Online Child Sexual Exploitation and Abuse, 2024 Bracket Foundation.

Brenner, J. (2019, Nov 25). *"The Deepfake Age: Who Gatekeeps Digital Trust?".* iProov. Retrieved Jan 29, 2020, from https://www.iproov.com/newsroom/blog/the-deepfake-age-who-gatekeeps-digital-trust

Bureau, T. H. (2024, -05–22T06:09:07.000). Stable Diffusion text-to-image tech allegedly used to create child abuse media and victimise a teenager. *The Hindu* https://www.thehindu.com/sci-tech/technology/stable-diffusion-text-to-image-tech-used-allegedly-create-child-abuse-media-victimise-a-teenager/article68202694.ece

Charlotte Child Pornography Case Shows 'Unsettling' Reach of AI Imagery. (2024, Apr 29). FBI. https://www.fbi.gov/news/stories/charlotte-child-sexual-abuse-material-case-shows-unsettling-reach-of-ai-generated-imagery

Clough, J. (2010). Principles of Cybercrime. Cambridge University Press.

Davy, D., & Lundrigan, S. (2024). *Artificial intelligence-produced child sexual abuse material: Insights from Dark Web forum posts.* https://www.weprotect.org/blog/ai-produced-child-sexual-abuse-material-insights-from-dark-web-forum-discussions/

Deepfake Detection Challenge Dataset. (2020, Jun 25). Meta. https://ai.meta.com/datasets/dfdc/

Detecting Audio Deep Fakes With AI. (2019, Sep 28). https://medium.com/dessa-news/detecting-audio-deepfakes-f2edfd8e2b35

Downing, S. (2024). The Role of AI in Child Exploitation Crimes. Journal of Cybersecurity, 8(1), 55-70.

Downing, S. (2024, Sep 6). *Unveiling the challenges of AI-generated CSAM.* CameraForensics. https://www.cameraforensics.com/blog/2024/09/06/unveiling-the-challenges-of-ai-generated-csam/

Europol, Trend Micro, and UNICRI. (Mar. 3, 2020). Criminal Misuse of AI and Deepfakes, The Hague, The Netherlands.

Gillespie, A. (2010). Child Pornography: Law and Policy. Routledge.

Gillespie, T. (2016). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press. https://books.google.ae/books?id=cOJgDwAAQBAJ&printsec=frontcover&source=gbs_ViewAPI&hl=en&redir_esc=y#v=onepage&q&f=false

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. & Bengio, Y. (2014, June 10). *Generative Adversarial Networks.* Retrieved Nov 12, 2024, from http://arxiv.org/abs/1406.2661

Greijer, S., & Doek, J. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. ECPAT International, 41.

Harris, M. (2019). AI and Deepfake Technologies in Media Production. Springer.

How AI is being abused to create child sexual abuse imagery, October 2023, PUBLIC VERSION, pp. 11–15.

ICTs and Sexual Exploitation of Children in Europe, László Dornfeld, Ferenc Mádl Institute of Comparative Law, Hungary.

International Watch Foundation (2021). Annual Report on Child Sexual Abuse Material. Internet Watch Foundation.

Jaiman, A. (2022, -08–02T21:55:28.894). *Deepfake harms and threat modeling.* Retrieved Jul 26, 2023, from https://towardsdatascience.com/deepfakes-harms-and-threat-modeling-c09cbe0b7883

Kaur, A., & Randhawa, P. (2020). Investigating Illegal Activities in the Dark Web. International Journal of Cyber Security, 7(3), 178-190.

Krishna, K., et al. (2024). AI-Generated Child Exploitation Material: New Trends and Challenges. Policing and Public Protection Institute.

Lapowsky, I. (2023, -06–24). The Race to Prevent 'the Worst Case Scenario for Machine Learning'. *The New York Times* https://www.nytimes.com/2023/06/24/business/ai-generated-explicit-images.html

Levine, T. R. (2014). Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection. *Journal of Language and Social Psychology, 33*, 378–392. https://doi.org/10.1177/0261927X14535916. https://www.researchgate.net/publication/273593306_Truth-Default_Theory_TDT_A_Theory_of_Human_Deception_and_Deception_Detection

Mahmud, B. U., & Sharmin, A. (2023). Deep Insights of Deepfake Technology: A Review., 13–15. http://arxiv.org/abs/2105.00192

Manke, K. (2019, Jun 18). *Researchers use facial quirks to unmask 'deepfakes'*. Retrieved Aug 26, 2020, from https://news.berkeley.edu/2019/06/18/researchers-use-facial-quirks-to-unmask-deepfakes/

Martínez, A. G. (2018, Mar 26). The Blockchain Solution to Our Deepfake Problems. *Wired,* https://www.wired.com/story/the-blockchain-solution-to-our-deepfake-problems/

Mehta, I. (2020, Sep 02). The Next Web. "Microsoft's new deepfake detection tool rates bogus videos with a confidence score." Retrieved 2020, Sep 08 from https://thenextweb.com/neural/2020/09/02/microsofts-new-deepfake-detection-toolrates- bogus-videos-with-a-confidence-score/

National Centre for Missing and Exploited Children. (2023). Cyber Tipline Statistics. NCMEC.

NetClean, NetClean Report 2019: A Report About Child Sexual Abuse Crime, 2019, at https://www.netclean.com/netclean-report-2019/

Ofusori, L. O., & Hendradi, R. (2023). Understanding the Impact of the Dark Web on Society: A Systematic Literature Review. *Nternational Journal of Information Science and Management, 21*(4), 8. https://ijism.isc.ac/article_708195_04c859319ede75bc0ba128fbd841bd64.pdf

OHCHR | Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment. (2024, Jun 05). Special Rapporteur on the sale and sexual exploitation of children. https://www.ohchr.org/en/calls-for-input/2024/call-input-existing-and-emerging-sexually-exploitative-practices-against

Olson, A. (2022). The Double-side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography. *Georgia Law Review, 56*(2), 874–877. https://digitalcommons.law.uga.edu/glr/vol56/iss2/8

Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws, 13*(6), 9–13. https://doi.org/10.3390/laws13060067

Patrini, G. (2019). Mapping the Deepfake Landscape-Deeptrace. *Retrieved July-23–2020 from* https://deeptracelabs.com/Mapping-the-Deepfake-Landscape

Poborilova, L. (2011). Virtual Child Pornography and Its Legal Implications. Journal of Information Law, 17(4), 241-246.

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J. & Nießner, M. (2019, August 26). *FaceForensics++: Learning to Detect Manipulated Facial Images.* Retrieved Aug 26, 2020, from http://arxiv.org/abs/1901.08971

Samantha, C. (2020). New Deepfake Method Can Put Words In Anyone's Mouth. *Tech by VICE, 24.* https://www.vice.com/en_us/article/g5xvk7/researchers-created-a-way-to-make-realistic-deepfakes-from-audioclips

Schwartz, O. (2018). You thought fake news was bad? Deep fakes are where truth goes to die. *The Guardian, 12*, 2018. https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

Shakarian, P. (2018). The Role of Black Markets in Cybercrime. Journal of Digital Forensics, 6(1), 87-99.

Spalevic, N., & Ilic, S. (2017). The Dark Web and Its Impact on Child Exploitation. Journal of Forensic Science, 3(2), 65-78.

Testimony of John Shehan. (2024). "Addressing Real Harm Done by Deepfakes". *National Center for Missing & Exploited Children,* https://www.missingkids.org/content/dam/missingkids/pdfs/final-written-testimony-john-shehan-house-oversight-subcommittee-hearing.pdf

Thiel, D. et al., Generative ML and CSAM: Implications and Mitigations, Stanford Internet Observatory, Jun. 24, 2023, at https://fsi.stanford.edu/publication/generative-ml-and-csam-implications-and-mitigations

Valle, G. D. (2024, May 21). *Wisconsin man arrested for allegedly creating AI-generated child sexual abuse material.* https://www.theverge.com/2024/5/21/24161965/ai-csam-instagram-stable-diffusion-arrest

Verma, P., & Oremus, W. (2023, Jun 26). Meta's new AI lets people make chatbots. They're using it for sex. *Washington Post* https://www.washingtonpost.com/technology/2023/06/26/facebook-chatbot-sex/

Vincenzo Ciancaglini, Craig Gibson, and David Sancho, Odhran McCarthy and Maria Eira, Philipp Amann and Aglika Klayn, *Trend Micro Research,2020* , 56- 60. https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf

Western District of North Carolina | Charlotte Child Psychiatrist Is Sentenced To 40 Years In Prison For Sexual Exploitation of A Minor And Using Artificial Intelligence To Create Child Pornography Images Of Minors | United States Department of Justice. (2023, Nov 08). United States Attorney's Office—Western District of North Carolina. https://www.justice.gov/usao-wdnc/pr/charlotte-child-psychiatrist-sentenced-40-years-prison-sexual-exploitation-minor-and

What has changed in the AI CSAM landscape? (2024). *IWF, Internet Watch Foundation,*, 22–25. https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf

What is Deepfake Technology and How Are Threat Actors Using It? (2023, Jun 1). FlashPoint. Retrieved Sep 20, 2023, from https://flashpoint.io/blog/what-is-deepfake-technology/

Will Douglas Heaven. (2020, Jun 12). *Facebook just released a database of 100,000 deepfakes to teach AI how to spot them.* iProov. Retrieved Aug 26, 2020, from https://www.technologyreview.com/2020/06/12/1003475/facebooks-deepfake-detection-challenge-neural-network-ai/

Yuezun Li, Ming-Ching Chang, & Siwei Lyu. (2018). [1806.02877] In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking. https://arxiv.org/abs/1806.02877

Investigating Children Sexual Abuse Cases in the Dark Web



Eldar Saljic and Dusko Tomic

1 Introduction

The digital era has witnessed an unprecedented surge in technological interconnectedness, ushering in transformative changes across various facets of human existence. Within this paradigm, the dark web has emerged as an enigmatic space that eludes conventional scrutiny, fostering an array of illicit activities. The door opener to the dark web was the TOR network, which aims to provide anonymity for its users by rerouting personal data through various nodes and connection points. Furthermore, the rise of cryptocurrencies after the 2008 financial crisis made it possible for marketplaces for the trade of illegal goods and services to be opened.

The most intricate emergence in the dark web is found on forums and pages that contain child abuse material or sexual material involving children and minors. Studies about child sexual material and child abuse material in the dark web, published in different timeframes (the 2000s, 2010s, and 2020s) all come to one conclusion, which is that child abusive sexual material (CSAM) is the most frequently shared content on dark web pages (Guerra & Westlake, 2023). Research on the surface web, which is the normal internet accessible through common browsers, showed that there are several millions of cases of child-abusive material being shared on common services, while the estimates on the dark web could be millions of times higher since the common web crawlers used to scan the surface web for such materials cannot be used in the dark web (Jardine, 2022).

This case study analysis aims to analyze several child abuse cases that were uncovered in the dark web. The research aims to provide different suggestions on the ways to detect and trace child-abusive material on the dark web more effectively in the future. Furthermore, the research aims to present recommendations for law enforcement regarding the preparedness to combat child-abusive material shared on

E. Saljic (✉) · D. Tomic
American University in the Emirates, Dubai, UAE
e-mail: dreldar.saljic@outlook.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_2

the dark web and to better understand how to operate in the dark web in undercover and indirect online investigations. Additionally, the research aims to present and depict the scale and extent to which child-abusive material is shared online. The research also aims to raise awareness about child-abusive material online and to present prevention ways for law enforcement and the public by presenting the modus operandi of predators online and how these predatorial groups operate.

1.1 Acronyms and Abbreviations

Surface web: the normally accessed internet through open browsers that do not protect the identity of the users and let information be accessed by all users.

Dark Web	Internet only accessed through the TOR network, is not indexed by surface web search engines, and does not have openly available information and domains and/or is not available for users of openly indexed internet.
Tor	The Onion Router—A specified browser used to access the dark web by rerouting the IP through certain filters, protecting the original identity of the users and the access points.
Open Source	Software that openly shares its source code with the public and the public can modify or indicate changes to the code in forums or websites.
CSAM	Child Sexual Abuse (Abusive) Material
VPN	Virtual Private Network
FBI	Federal Bureau of Investigation
IP	Internet Protocol (Internet Protocol address), a unique Internet Protocol address that reveals the location and the identity of the computer used to access the Internet.
H2TC	Hurt to the core, a dark web site that hosted violent CSAM
NGO	Nongovernment organization
AI	Artificial Intelligence

2 Literature Review

This chapter includes an overview of the literature analysis used for this research. The research reviewed literature connected to the general issues of the dark web, and literature sources analyzing the problem of child sexual abuse on the dark web and including the description of the cases as well. In this chapter, the research included a short description of the sources reviewed and the impact they had on the research itself.

For the general description of the dark web and the security concerns connected to it, this research referred to Chertoff (2023), who presented a public policy perspective

of the dark web. Chertoff (2023) hints toward the security concerns of the dark web because it provides high anonymity for the users. According to the author, the dark web offers opportunities for communication between journalists and activists in countries where free speech and the internet are hindered. However, it also allows anonymity to more serious offenses and illegal communities to form, some of which include marketplaces for drugs, arms, and other illegal goods and services, as well as forums and websites hosting sexually abusive content of children and adults. The anonymity provided by the dark web attracts individuals who hide their true intentions from society, and law enforcement must create methods and practices to stop more abuse and illegal actions that may arise from the popularity of such websites (Chertoff, 2023). The author also has another research published in 2021, which describes one of the cases analyzed in this research. Further details are revealed in later sections, which were directly taken by Chertoff and Jardine (2021) and their description of the *Playpen* case (Chertoff & Jardine, 2021). Complementary research to Chertoff (2023) and Chertoff and Jardine (2021) is Davis and Arrigo (2021), where the anonymity techniques in the dark web are described. The source offers insight into certain techniques to how the dark web shrouds and protects the privacy of its users, while also not being vulnerable to the techniques of law enforcement. It was used to provide further insight into the previously mentioned sources and offer further details into it.

Another source used to present the different cases analyzed in this research comes from Akhgar et al. (2021), which provided a collection of child abusive cases found on the dark web. Certain cases were extracted and analyzed in later sections. The research results provided by the authors provided great insight into the nature and the modus operandi of dark web perpetrators, and hint toward the large scale and the challenge to security connected to the large number of cases of illegal content found on the dark web (Akhgar et al., 2021).

Guerra and Westlake (2023) researched the main traits of websites hosting child-abusive contexts on the dark web. The focus point of the authors was to recommend improvements to automatic detection systems for websites containing child-abusive content, as well as to point out the vulnerabilities of such systems. Furthermore, the paper aimed to identify patterns in the hosting structures of the websites and the naming practices for hosting folders to improve the detection of the internet for child-abusive content (Guerra & Westlake, 2023). The authors suggested that there is a large volume of child-abusive content to be found not just on the dark web, but also on the surface web. Additionally, the large volume of such content being present online is a major challenge for law enforcement and severely limits the ability of law enforcement to detect such content online. In the year 2019, more than 15 million reports were made by more than 100 service providers (Guerra & Westlake, 2023). The research concluded that websites providing file hosting services need to be evaluated more in the detection of child-abusive content. Furthermore, these websites appeared to show child-abusive content right in the hosting directories and in most files. Furthermore, file and folder names should be combined with the detecting algorithms to improve the detection of child-abusive content online (n.d.). This paper was valuable for the research because it provided insight into the quantity

of child-abusive content online and the overwhelming number of reports automatic detection systems received.

Another paper by the same authors presents detection tactics on the dark web for the detection of child-abusive content in a better detail. The authors hint that by researching and exploring the names of files and folders, as well as the structuring of files on hosting websites on the dark web can reveal hints of child sexual abusive content online (Westlake & Guerra, 2023). The authors concluded that manual search and investigation cannot meet the quantity of content found online, especially on dark web hosting pages. Therefore, tools can be created for the automatic detection of dark web pages, which would search for keywords, but should also search for file structures and folder names that might reveal hints for the detection of child-abusive content. However, dark web pages are disconnected from other web pages (other than on the surface web), which leads to the conclusion that detection tools must be improved because the number of contents found online is overwhelmingly large (Westlake & Guerra, 2023). This paper is valuable for the research because it presents the ultimate problem of the number of child-abusive content on the dark web, and allows insights into the frame of the problem of child abuse.

The above-mentioned research corresponds with Chiang (2024), who researched the performance and knowledge of fresh offenders on child abusive websites. According to the author, the scale of child-abusive content on the dark web forums overwhelms law enforcement offices on a national and global scale (Chiang, 2024). As such, the situation allows new websites to be created and new communities to arise. As Chiang (2024) states, connected research detected more than 4 million websites hosting child-abusive content on the internet, with the number increasingly rising. The author researched how the users in such forums communicate with each other and what terminology new users use when communicating with older and/or more experienced users. Additionally, the research found that users of such forums can be distinguished into fairly new users who are just starting to explore the content, most of which express their appreciation for such communities and are willing to state their motivations, and alignment with the content (Chiang, 2024). The research concluded that law enforcement on the national and international levels must improve their detection techniques and their research techniques since such communities are among the largest found on the dark web. Furthermore, the users are self-aware and are aware of the content and the experiences they exchange with other users, which means that these communities are confident in their existence and wish to normalize their preferences (n.d.). The demographics of the users include members of large communities, some of which do have children themselves, which makes it even more alarming and puts enormous pressure on law enforcement to enhance their investigations and detection techniques because the amount of content and users hints toward a potentially large number of victims which remain undetected.

Demetis and Kietzmann (2021) researched the problem of online child abuse in the context of security challenges. The authors found that the internet, especially the dark web, allows pedophile predators to communicate with each other and share content in online communities. The criminological research focuses only on the criminal aspect of child-abusive content online, which leaves a gap in the exploration of such criminal

behavior, where less attention is paid to those who organize such communities and make sure that other communities arise as soon as law enforcement manages to take down several communities (Demetis & Kietzmann, 2021).

Wang et al. (2023) investigated the availability of content material found on the dark web and the dark web markets. The research paper found that the content and the sales of child-abusive materials on the dark web increased almost tenfold in the last decade, with more than ten thousand items listed each day for sale on dark web markets (Wang et al., 2023). The paper concludes that the items connected to child abuse and child exploitation are increasing on dark web markets, calling for law enforcement to increase the presence and detection methods for such dark web markets since every item sold has one or more potential victims. Such markets are well organized and are aware of the content and materials that are being sold, hinting at the normalization of such material in the dark web (Wang et al., 2023).

2.1 Impact of Encryption and Tools on CSAM Investigations

Van der Bruggen and Blokland (2021) researched the organization levels of child abuse communities on the dark web. The research hinted that child-abusive content is the most popular content shared on the dark web, with 80% of dark web traffic being generated by child-abusive websites only (van der Bruggen & Blokland, 2021). The research found that websites of child-abusive content are highly well-organized and function similarly to websites providing legal content on the surface web. The two authors have another research connected to this paper, presenting the profiles of dark web sexual abusers in 2022. In this research, they presented the findings that profiles of child-abusive forum users vary from young adults in their mid-20s or 30s, and even people who have families and even have children themselves, finding that pedophilia is widely spread across the world and attracts far more users, which were able to provide insight into the large number and the scale of the problem of child abuse (van der Bruggen & Blokland, 2022). Such a large variety of users and such a large amount of content being shared present child abuse as a highly complex problem and a high challenge for law enforcement authorities.

Dalins et al. (2022) investigated the motivation for perpetrators to exchange their experiences on the dark web. The research found that, like serial killers and other criminal offenders, people seek an outlet to re-live the excitement and the experience to satisfy to receive satisfaction. Furthermore, people are more likely to shroud themselves in anonymity and exchange with like-minded people under anonymity than they are to meet in person or commit physically abusive behavior (Dalins et al., 2022). The researchers concluded that people who are discussing and enjoying illegal content online can become perpetrators themselves to achieve status on those dark web online forums. Furthermore, other criminal acts can be connected to just one type of crime—often, there is identity theft, and theft of intellectual property (when photographs are stolen from social media accounts). According to the researchers,

this is a real security challenge because it can affect any member of society, starting with small children and going through all demographics (Dalins et al., 2022).

A criminological perspective into child sexual abuse on the dark web is being provided by Fortin and Paquette (2022). The paper presents examples of the sexual online abuse of children and states that the number of reported use cases of theft from social media and manipulation of photos of children posted on social media, which were then resold on the dark web markets and spread in dark web forums in the light of child sexual abuse reaches into the millions, with communities urging parents not to share pictures of their children online and protect the identity of them to protect them from being made into objects of sexual gratification online (Fortin & Paquette, 2022). According to the researchers, members of dark web forums with child-sexualized materials are often scanning social media pages for non-sexual pictures of children that can be used in dark web forums. These pictures are often manipulated and modified to represent a more sexual context. Therefore, the paper concludes that not only does law enforcement have to improve their detection and investigation methods, but also the parents and the public must be made aware of the security concerns and must be taught to protect children from such abuse cases (Fortin & Paquette, 2022).

Chopin and Decary-Hetu (2023) explored the context of criminality in online pedophile communities and aimed to understand the decision-making processes of sexual offenders on the internet. Additionally, the research aimed to explore the aspect of cybersecurity in dark-web pedophile forums and the light of the users of such forums (Chopin & Decary-Hetu, 2023). The researchers found that users of dark web child abuse forums were less and less concerned about their cybersecurity, mainly because the dark web provides certain anonymity to the users. Furthermore, users of such forums are aware of the large number of forums on the surface web and that the security officers and researchers are overwhelmed in the discovery of child abuse forums, which, in return, provides the users of dark web child abuse forums with a certain aspect of security (Chopin & Decary-Hetu, 2023). The findings of this research were important for this research, since they provide an insight into the modus operandi and the mindset of child abuse forum users, as well as the awareness of the existence of other forums and the fact that security services are dealing with a large number of offenders and forums, which makes the discovery and shutdown of every forum on the dark web seem an impossible task (Chopin & Decary-Hetu, 2023).

Gannon et al. (2023) researched the development of the dark web and its implications for the digitalization of society and the implication for the development of CSAM (child sexual abuse material) forums. The research found that historically, people sexually attracted to children started gathering in physical so-called “support groups” and were trading illegal pieces of CSAM in adult stores and so-called “book clubs” during the 1970s and the 1980s. However, as policing improved in the 1990s and law enforcement was able to better track and prosecute these individuals, these gatherings and support groups became more and more secretive. With the introduction of the internet in the early 2000s and the rise of the dark web later on, adults attracted to children were organizing themselves in such forums and started sharing

CSAM on the dark and the surface web (Gannon et al., 2023). The anonymity of the dark web and the global access to it led to an exploding number of forums with CSAM. Europol commenced with *Operation Rescue* cooperation with 13 other security forces and recorded more than 600 identified suspects, more than 170 arrests, and ca. 230 children rescued from sexual predators (Gannon et al., 2023). In comparison, CSAM websites are 2000 times more likely found on the dark web than on the surface web (n.d.). Furthermore, the dark net websites containing CSAM are not indexed in dark web wikis but are much more private and most likely shared through private invitations. The forum users themselves do see the criminality of their presence but lack a fundamental understanding of the criminality of their sexual attractions. In their opinion, their sexual behavior should be normalized. Furthermore, they assume that children can enjoy sexual acts and indicate that children also "benefit" from sexual experiences. Their further behavior is completely neutralizing the criminal and offensive nature of their desires. The research suggests that law enforcement must prioritize and allocate most of its technological resources for the discovery and detection of such forums. Furthermore, they must place targeted posts in these forums providing help for everyone who wishes to stop their behavior and wishes to seek help and treatment for the condition they have. Finally, the researchers indicate that there is an absence of research that aims to understand the risks and the profiles of CSAM forum users and create interventions that prevent the desire to become a member of such forums. When the users are better understood, law enforcement agencies will be able to better address the risks and protect children that are found on CSAM forums (Gannon et al., 2023).

Insoll et al. (2022) investigated the risk factors behind the users of CSAM forums that contact children online directly. The researchers created a survey aimed at helping users of CSAM forums and analyzed the behavior and the first contacts with users and CSAM material. According to the researchers, the use of CSAM has become a global problem, with Interpol reporting more than 2 million pieces of material showing child sexual abuse, with the number of materials doubling between 2019 and 2020 (Insoll et al., 2022). Furthermore, the true extent of the problem remains unknown. The conclusions of the research have provided significant insights into this research, showing that most users of CSAM forums on the dark web come in contact with such materials accidentally and that the desire to be attracted to children has been felt since their adult years. However, it mostly develops between the age of 18 and 26. Most of the users over the age of 30 or 40 report that they first started exploring attraction to children between the ages of 18 and 26. Additionally, the research implicates that such forums must be regularly frequented by law enforcement agencies since there is a direct link between consuming CSAM on the dark web and the direct seeking of contact with children for sexual acts on the surface web and the dark web (Insoll et al., 2022).

Leclerc et al. (2022) analyzed how offenders operate in dark web forums with CSAM. By interviewing online investigators, the study aimed to reconstruct how offenders operate and give implications on how to fight child abuse on the dark web and how to prevent it (Leclerc et al., 2022). The researchers identified three phases in which offenders operate before and after they get involved in dark web forums

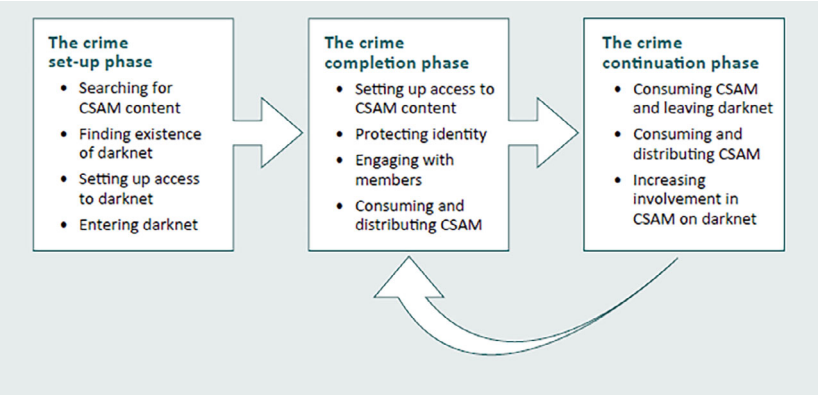


Fig. 1 CSAM offenders' modus operandi in 3 Phases (Leclerc et al., 2022)

presenting CSAM. In the first phase—the "set up phase", the offenders begin with different motives (sexual desire to explore minors and validate their sexual interests). The second step within this phase includes the search for peers' and interests' websites on the surface web, where the indications will lead the offenders toward the dark web (Leclerc et al., 2022). The offenders receive information that the dark web will protect their identity and will protect them from law enforcement investigations (other than from the surface web). The second phase of the operation is called the "crime completion phase", where the offenders have already secured their access to the dark web and registered themselves within such forums. They also quickly start engaging members of the forum and consume and/or distribute CSAM themselves. The third phase is quickly entered and represents a circulation between the second and the third phase. Offenders are either consuming CSAM and leaving the forums soon afterward or getting more involved within forums and becoming distributors of CSAM themselves (Leclerc et al., 2022). The phases of involvement are presented in the following Fig. 1.

Leclerc et al. (2022) made clear that the research provides an outline of how most offenders operated according to the data collected by law enforcement agents. However, the research also says that the development of offenders and CSAM forum members of the dark web can also occur non-linearly. Some offenders may not search the surface web because they are in some form connected to certain individuals who are already members of forums and can guide them through the process. However, Leclerc et al. (2022) presented a framework for global offenders that might not be affiliated with like-minded individuals and seek their information on the internet. Since both the surface web and the dark web can be accessed worldwide, the problem of CSAM forums loses its borders and becomes a worldwide problem. Therefore, the researchers call for all international organizations to create a more data-oriented culture and set up systematic processes that would evaluate and analyze data in search of potential offenders (Leclerc et al., 2022). The processes presented should be examined step-by-step, which would lead to the discovery of certain actions taken

by offenders. These evaluations should also be included in cybercrime training and all forms of digital investigations since CSAM makes up a significant portion of criminal activities on the dark web. For the researchers, the biggest acknowledgment that must be made is that CSAM forums will not disappear from the dark web any time soon, regardless of how sophisticated online investigations will become (Leclerc et al., 2022). However, mapping the steps presented and collaborating with other online investigators and law enforcement agencies worldwide would be beneficial in tracking individuals and closing CSAM forums before they can move on to the next sites. Additionally, the researchers state that a society registering the given steps and socially deviant behavior would be beneficial in the fight against CSAM forums and child abuse in general since this would lead to faster detection without the necessary involvement of law enforcement (Leclerc et al., 2022).

This research was of high importance for this case study analysis since it provided a guideline and structure in which the cases of this analysis will be analyzed and separated. Therefore, this case study analysis used the model given by Leclerc et al. (2022) for the structuring of the case study analysis and identifying the above-given steps in the cases analyzed.

Shobana et al. (2022) discuss the use of artificial intelligence in the fight against CSAM on the dark web. The research presents a significant topic for this case study analysis since it provides aspects to a case discussed in the later chapters and presents a solution on how to combat CSAM materials and find offenders on dark web forums with CSAM (Shobana et al., 2022). The research compared an autonomous AI detection system for evaluating and detecting CSAM offenders to a human-led approach in combating CSAM by using AI. It found that autonomous AI detection systems have certain disadvantages, mainly that they cannot distinguish between websites hosting adult sexual content and cannot identify persons with sexual intents. Furthermore, autonomous systems can only be applied to the surface web and must be evaluated by humans, which would only add to the complexity of the investigation. On the dark web, where most of CSAM is being distributed and created, autonomous artificial intelligence still cannot be applied (Shobana et al., 2022).

However, another aspect can be used in the creation of avatars. Artificial Intelligence has become so sophisticated that it can create so-called *deepfakes*, videos depicting real-time characters (mostly celebrities) saying and doing various sorts of things, most of which are untypical for these individuals. Therefore, the researchers find that AI models can be used to detect persons interested in CSAM to evaluate and detect their identities. These models can be applied in the dark web as well and they can be used to assure the offender that he is talking to a seemingly real minor, further assuring offenders and making them feel safer in the investigation (n.d.). The paper concludes by stating that AI must be used proactively to combat CSAM and to attract predators, which would offer immense help with combating child abuse and the material being posted on the dark web. This source had a large impact on this case study analysis since it offered a different view of different approaches to combating the said phenomenon of CSAM on the dark web and will be a focus point in the discussion following the case study analysis.

2.2 Emerging Detection Technologies and Limitations

Emerging detection technologies for combating child sexual abuse material (CSAM) on the dark web are pivotal in addressing the growing exploitation challenges posed by anonymity and encryption. These technologies leverage advancements in artificial intelligence (AI), machine learning (ML), and blockchain analysis to identify, track, and mitigate the dissemination of CSAM. AI-driven tools are particularly effective in analyzing large datasets to identify patterns indicative of abuse materials (Demetis & Kietzmann, 2021). Deep learning models, trained on legally approved datasets, can detect specific image or video features associated with CSAM, enabling law enforcement to pinpoint illicit content with increased precision. Additionally, natural language processing (NLP) algorithms are utilized to monitor forums and chats for grooming behaviors or trafficking indicators (Kokolaki et al., 2020).

Blockchain analysis tools are critical for tracing cryptocurrency transactions linked to dark web marketplaces. These tools use sophisticated algorithms to de-anonymize blockchain transactions, mapping them to known patterns of illicit activity and aiding in tracking perpetrators. Furthermore, innovations in digital watermarking and hashing allow for the creation of unique signatures for known CSAM files, enabling their swift identification and removal, even if attempts are made to modify them (Chiang, 2024).

Privacy-preserving approaches, such as federated learning, ensure that detection mechanisms can operate without compromising the privacy of innocent users, a critical consideration in combating exploitation on platforms offering end-to-end encryption. Meanwhile, partnerships between tech companies and non-profits, like those developing tools under the National Center for Missing & Exploited Children (NCMEC), enhance collaborative efforts in real-time reporting and takedown of CSAM (Demetis & Kietzmann, 2021).

Emerging technologies are also pushing for enhanced predictive analytics, which can identify high-risk behaviors or regions prone to exploitation. Despite their promise, these tools face ethical and legal challenges, such as balancing user privacy with surveillance needs. Continuous innovation and collaboration are essential to evolving these technologies into robust shields against the proliferation of CSAM on the dark web (Dalins et al., 2022).

2.3 Legal and Ethical Considerations

Despite being a highly important task in policing and combating CSAM on the Dark Web, the investigations must follow legal and ethical considerations. These ensure that efforts to combat illicit activities, such as drug trafficking, human trafficking, and the distribution of child sexual abuse material (CSAM), align with fundamental rights and the rule of law. One of the primary legal challenges lies in navigating jurisdictional issues. The dark web operates across international borders, making

it difficult to determine which country's laws apply and requiring seamless cooperation between global law enforcement agencies. Investigators must also ensure compliance with laws governing privacy and digital rights, as unauthorized surveillance or hacking can violate constitutional protections and lead to evidence being inadmissible in court (Akhgar et al., 2021).

Ethical concerns often revolve around the methods used to infiltrate dark web networks. For example, law enforcement agencies sometimes deploy honeypots or engage in undercover operations that may blur ethical boundaries. While these methods are effective in identifying perpetrators, they must be carefully managed to avoid entrapment, where individuals are coerced into committing crimes, they might not have otherwise engaged in. Additionally, the use of advanced surveillance technologies, such as artificial intelligence and machine learning algorithms, raises concerns about bias, overreach, and the potential for misuse. Algorithms must be transparent, accountable, and free of discriminatory biases to ensure ethical use (Davis & Arrigo, 2021).

Another ethical dilemma arises in the balance between public safety and individual privacy. Investigators often rely on techniques that involve breaking encryption or tracking online activity, which can inadvertently expose innocent users to unwarranted scrutiny. The principle of proportionality is essential, ensuring that investigative methods are commensurate with the severity of the crime being pursued.

Furthermore, the retention and use of data collected during investigations present additional challenges. Strict guidelines must govern how this data is stored, who has access, and how long it is retained, preventing misuse or breaches that could compromise personal information. Ultimately, dark web investigations require a delicate balance between aggressive pursuit of justice and adherence to legal and ethical standards. Transparent oversight, robust legal frameworks, and ongoing ethical evaluations are essential to maintaining public trust while effectively addressing dark web criminality.

3 Methodology

This chapter presents the methodology applied to the case study analysis and how the analysis reaches its conclusions and recommendations.

This research adopts a case study approach due to its effectiveness in exploring complex and sensitive phenomena such as child abuse in the dark web. Case studies allow for an in-depth examination of individual cases, providing valuable insights into the context, dynamics, and impacts of the phenomenon. The researcher employs an exploratory case study design, aiming to investigate the nature and extent of child abuse occurring within the dark web environment. The exploratory nature of the research facilitates a deeper understanding of the underlying factors contributing to the prevalence of such abuse.

The unit of analysis in this study is individual cases of child abuse identified within the dark web. Each case represents a unique instance of abuse, allowing for detailed

analysis and interpretation of the associated factors and dynamics. The cases studied in this research are selected based on their relevance to the phenomenon of child abuse in the dark web. A purposive sampling approach is employed to ensure that the selected cases provide meaningful insights into the various aspects of the issue.

Secondary sources are utilized in this study, including peer-reviewed journal articles, books, and credible web pages. These sources provide a rich and diverse range of information about the cases of child abuse within the dark web. The information collection process involves a systematic review and analysis of relevant literature and online resources. Information related to identified cases of child abuse, including case descriptions, perpetrator profiles, victim characteristics, and legal implications, is extracted and synthesized for further analysis. A comprehensive search strategy is employed to identify relevant literature and online sources related to child abuse in the dark web.

Limitations of this study include the reliance on secondary data sources, which may be subject to biases, inaccuracies, and incompleteness. Additionally, the dynamic and clandestine nature of the dark web presents challenges in accessing reliable and comprehensive information. These limitations may affect the depth and scope of the analysis, potentially leading to gaps or inconsistencies in the findings. However, efforts are made to mitigate these limitations through scrutiny and validation of the collected data.

This methodology chapter outlines the research approach adopted in the study of child abuse in the dark web. By employing a case study analysis and utilizing secondary data from various sources, the research aims to provide valuable insights into this complex and concerning phenomenon. Ethical considerations are paramount throughout the research process, ensuring the responsible and respectful treatment of sensitive information. Despite certain limitations, this study contributes to the existing body of knowledge on child abuse prevention and intervention strategies within the digital landscape.

4 Case Study Analysis

This chapter presents the main body of the analysis. It presents the analysis of three cases of child sexual abuse on the dark web, including the Playpen case, the case of Matthew Falder, and the case of Operation Sweetie (Ngo et al., 2024). Furthermore, the cases are analyzed in the steps provided by previous research and will analyze similarities and special aspects of the modus operandi before continuing into the discussion and concluding the case study analysis.

4.1 Playpen

As mentioned previously in the research, law enforcement has begun actively tracking down CSAM websites on the dark web since they make up a significant portion of the dark web (S. & Randhawa, 2020). Playpen is the name of a CSAM dark website that became one of the biggest CSAM dark web cases in the mid-2010s. In this case, international organizations worked together and managed to arrest more than 300 individuals who were connected to the website worldwide (Akhgar et al., 2021). Furthermore, the National Centre for Missing and Exploited Children (NCMEC) states that during the existence of the website, users viewed more than 20 million videos, images, or live streams with CSAM (Chertoff & Jardine, 2021).

The site was launched in August of 2014 by Steven Chase of Florida and quickly gained a larger following and gained the attention of law enforcement investigators (Shobana et al., 2022). However, due to the complexity of the TOR network and the hidden nature of dark web pages, investigators could not move forward into revealing the identity of the administrator and the location of the server hosting the webpage (Raven et al., 2021). Law enforcement agents did have indications that the website was gaining users rapidly, but they were only able to infiltrate the website and evidence the growing amount of material being posted to the website. To better infiltrate the website, the FBI deployed a hacking tool called NIT (Network Investigative Technology), which exploits a weakness in the TOR browser that is based on Mozilla Firefox, an open-source technology that openly shares the code for its web browser online and can be modified by different users (Davis & Arrigo, 2021). However, the NIT techniques require a certain target so that it can infiltrate everyone who uses or accesses the website and reveal its identity.

The deciding event happened in December 2014, when an undisclosed foreign law enforcement agency informed the FBI that a website they observed appeared to be misconfigured and showed the public IP of the computer performing the hosting (Chertoff & Jardine, 2021). The location of the server appeared to be in the United States of America, and the FBI quickly identified the website and infiltrated the webpage, revealing that only 4 months after the site had been set up, Playpen hosted more than 200 thousand members and that more than 100 thousand posts with pictures, videos, and links to other CSAM forums or postings with guidelines as to how to approach minors or how to perform illegal acts to minors (Akhgar et al., 2021).

After obtaining the search warrant and the necessary warrants for the arrests, the FBI arrested Steven W. Chase in Florida in February 2015 but kept the website running to infiltrate all the users who were active on Playpen. The operation was widened out internationally through cooperation with Europol and Interpol. It was called “Operation Pacifier” and led to more than 300 arrests in the United States of America, and more than 500 international arrests, with the identification of more than 50 children in the United States of America and their rescue from the abusers. One of the most shocking facts in Operation Pacifier was that most of the victims were abused by their parents (Chertoff & Jardine, 2021).

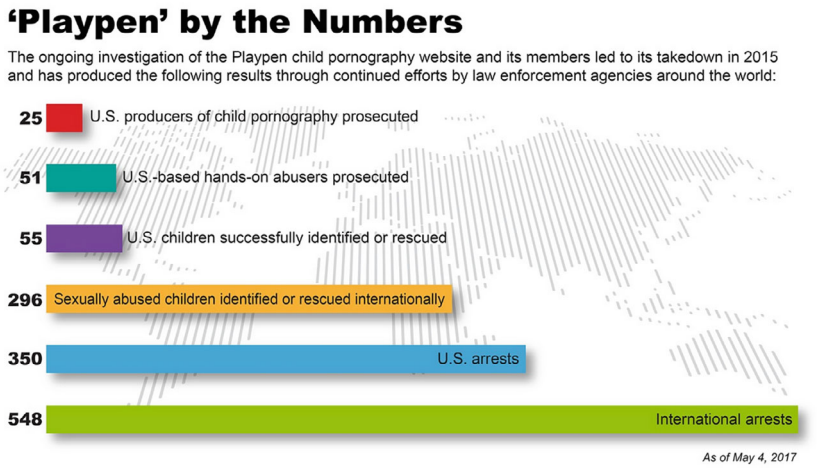


Fig. 2 Aftermath of Playpen and its consequences from 2017 (Chertoff, 2023)

Additional people arrested after Chase were David Lynn and Michael Fluckinger, all three middle-aged men with little to no connections to information technology or advanced knowledge in the operation of websites and the setup of complex dark web operations. Furthermore, it was revealed that they did not have prior convictions connected to sexual abuse or sexual abuse of children but had misdemeanors in the past (Akhgar et al., 2021). Additional arrests of users happened in Ireland, Slovakia, France, Spain, Italy, Croatia, Colombia, Switzerland, Malaysia, Peru, and Canada. The following graph shows the extent of Operation Pacifier and its impact until 2017 (Fig. 2).

The aftermath of the case had certain legal and ethical controversies bound to it, with the legal implications still being felt today. Certain courts and defenders argued that the seizure and the obtaining of the materials were unlawful and used infiltration techniques that are deemed unconstitutional by the U.S. justice system, while the courts themselves accepted the evidence in good faith, acknowledging the purpose of actions for the conviction and protection of further child abuse.

Analyzing Playpen through the 3 steps of the above-mentioned modus operandi of CSAM forum users, one can conclude that there is a significant first step, which starts with setting up the website called Playpen directly on the dark web and then continuing with the access and identity protection of the website. The continuation phase is also present with the Playpen attracting more and more users as time goes by. It can be noted that the identity of the administrators remained protected, but there was a lack of expertise or deeper knowledge of information technology, which hints that websites on the dark web are easy to create and set up. Ironically, it was exactly the lack of technological knowledge that probably led to a misconfiguration of the server and the IP address becoming visible. Furthermore, a deeper analysis of the Playpen case shows that the crime completion and the crime continuation phase would have most likely continued if the authorities did not step in. Had there also

not been investigators who were actively scanning the dark web for CSAM, Playpen would probably have grown to be the largest online community for CSAM, further continuing the criminal offense of child abuse, and further widening the large scale and extent of child sexual abuse.

4.2 Matthew Falder

The case of Matthew Falder is a case of one of the biggest websites for a sub-community of CSAM dark web pages, which is also called "hurt core". Hurt core is the form of CSAM that depicts violent acts such as rape, execution, physical dismemberment, or psychosocial abuse suffered by children. This case perfectly displays the production, sharing, and viewing of CSAM on the dark web (Kokolaki et al., 2020). Furthermore, it confronts researchers with individuals who understand technology and can secure themselves against investigators on the dark web, resulting in the website existing online for a very long time.

The investigation leading to the arrest of Matthew Falder started in 2013 when the FBI and other law enforcement agencies started hosting miscellaneous websites on different dark web hosting services to get information about the traffic for other dark web sites on the same servers. Soon enough, the FBI started noticing the increasing traffic and the existence of a website called "Hurt to the Core". The website registered more than 300 accounts and more than 100 posts daily, all of which related to sadism, torture, blackmail, humiliation, and rape (Chertoff, 2023). One profile titled "inthegarden" stood out with its activities, sharing regular posts on the topic of blackmail of an underaged girl (n.d.). According to investigators, the origin of the posts and the language used hint to a person from the United Kingdom, and the FBI informed the National Crime Agency (NCA) in the UK (van der Bruggen & Blokland, 2022).

Parallel to the activities of "inthegarden", another account named "666devil" has been as active as the prior. Specifically, the user "666devil" had a profile picture depicting an underaged girl. The user had claimed that the girl depicted in the picture was their daughter and that they were deliberating about how they could torture and abuse their daughter in an upcoming event called the "hell week" (Chertoff & Jardine, 2021). The user "666devil" had created a forum post collecting ideas of torture and making other users aware that they could make requests and receive graphic material in return (n.d.). Furthermore, the two accounts were linked with a third profile called "evilmind". The topics shared from the three profiles were similar, mostly discussing humiliation and blackmail of underaged victims who were forced to perform sexual or humiliating acts (Akhgar et al., 2021).

The three interconnected accounts collected, collated, and sold CSAM to several forums, including H2TC (Hurt to the Core), for acknowledgment and appraisal of other forum users. Materials shared by the above-mentioned profiles included auto-sexual acts of minors, and humiliating acts such as eating excrement, waste, or hurting themselves. The forum H2TC had created a game-like ranking system that awarded

points for the severity of CSAM and other content the users shared, with some areas of the forum only being able to be accessible after users had gained several points (Fortin & Paquette, 2022). For their content, the user received the title of "VIP Rapist" in the forum H2TC and continued posting stories and graphic materials continuously for more than 3 years. Falder was able to avoid detection and identification because he was well-versed in technology and used advanced encryption techniques to encrypt files and identities when sharing materials (Akhgar et al., 2021). These measures were tightened by Falder after two suspects from Australia were arrested for sexual acts against children in 2016. That year, Pete Scully and Matthew Graham were arrested in the Philippines and Australia for distributing CSAM and hurting core CSAM material. Graham had been using the nickname "Lux" and was the founder of H2TC. Graham also went public in 2013. Although anonymous, he spoke about CSAM dark web forums and stated that they are sure they cannot be detected due to them being well versed in technology, Graham himself being a student of Nanotechnology. Scully was arrested after sharing the video series "Daisy's destruction" on H2TC and various other forums, which is titled as one of the most gruesome depictions of hurt core CSAM. Scully was arrested in the Philippines in another investigation after concerned viewers informed authorities that they could trace back the race of the young girls depicted and local law enforcement in the Philippines started collaborating with Australian authorities to uncover the perpetrator (Owens et al., 2023).

The accounts on H2TC, later revealed to be Falder, talked about how they were recording their friends and family in private and intimate spaces without their consent, and all among each other distributed the "Pedo Manual", which was written by another user of H2TC and the former "Pedo Empire", closely tied to previously mentioned Graham and Scully, John Huckle, who was arrested in the Philippines and killed in prison by another inmate (Fortin & Paquette, 2022). After the identities of Scully, Huckle, Graham, and others were revealed, police went after a report made by a teenage girl in the UK, stating that the person had falsely identified themselves as an underaged girl and responded to advertisements on the advertisement board *Gumtree*. This report was made at the end of 2015 and involved a 16-year-old girl and someone responding to their babysitting advertisement. The offender has moved from communicating on the open platform gumtree to encrypted platforms such as WhatsApp or email. It was a request for a nude photograph that would be used in an artwork. After not consenting to the exchange, the account sent the victim graphic CSAM material and threatened to expose the victim as having CSAM on their devices (Chertoff, 2023). The victim provided the NCA with information about the account name used and the surface web emails connected to the accounts. With this information, NCA was able to collect information about 40 more victims and determine the identity of the girl in the profile of "666devil", which established a connection between the offender reported and the person using the account on H2TC. The Gumtree account was connected to a person in Birmingham, later revealed to be the university professor Matthew Falder (Chertoff & Jardine, 2021).

The NCA started covertly following Falder and filmed him using his laptop to post CSAM on dark web pages while riding in a train and Falder was arrested in 2017 at the University of Birmingham. The authorities found incriminating materials on

several drives titled "BM", which should have served as an acronym for "Blackmail" most likely. Furthermore, it was revealed that Falder was also recording his friends and family and had materials distributed on the dark web and to the victims of his blackmail schemes. After 3 days of questioning, Falder confessed to all the offenses in the UK, Australia, and the USA, and revealed his connection to the forum like H2TC (Chertoff & Jardine, 2021).

Contrasting the Matthew Falder case through the modus operandi model of Leclerc et al. (2022), one can see that Falder was highly intelligent and understood the methods used and the possibilities offered by the dark web. Further reports indicate that Falder held a PhD in science and worked as a university professor in Birmingham, further leading to the explanation of how he was able to avoid detection for such a long time. Furthermore, it was clear that Falder already had a tendency to perform evil acts against his friends and family members, but that the detection of the dark web had presented him with the opportunity to deepen his evil fantasies. Since the operation started in 2013 and Falder was arrested in 2017, it shows that once such individuals start with criminal behavior, they do not stop and gain a sense of confidence in their actions since they are protected through encryption and hiding measures by the TOR network.

The case of Matthew Falder shows how complex investigations of law enforcement agencies can lead to successful arrests of some of the most gruesome individuals. Furthermore, it highlights the need for law enforcement agencies to encourage the public to report any form of suspicion in online behavior they come across since some small misdemeanors can lead to deeper personalities and the detection of worse crimes. Furthermore, these methods must be improved by law enforcement to stop the spread of such material and abuse suffered by children in a much shorter time (Guerra & Westlake, 2023).

4.3 Operation Sweetie

Compared to the previous two cases, Operation Sweetie was an innovative operation created to catch pedophiles and sex offenders on the dark web which sought to interact with minors through webcam in a practice called "webcam sex tourism". Sex tourism is a phenomenon where individuals travel to different countries solely for sexual gratification. In its basic form, sex tourism occurs when individuals travel from countries with tight legislation about sodomy and prostitution to countries where prostitution is legal, and they would not be prosecuted for visiting brothels. Germany, the Netherlands, France, Russia, Ukraine, Slovakia, Hungary, and the Czech Republic receive sex tourists who visit legally owned and operated brothels. Southeast Asia also received sex tourists from Europe and the United States of America (Kloess & Van der Bruggen, 2023), mostly in the Philippines, India, Thailand, and Myanmar. However, sex tourism has also been under investigation due to a much darker side, which is sex tourism for the goal of performing sexual acts on teenagers and children, often children from impoverished neighborhoods with the promise of food and shelter.

The deviation "webcam sex tourism" removes the requirement of physical presence and places sex tourists on the internet, where offenders would require sexual acts to be performed in a video chat in front of a web camera (Chertoff & Jardine, 2021). The true extent of CSAM and webcam sex tourism is believed to reach more than 700 thousand users of CSAM dark web forums and over 40 thousand CSAM dark web forums offering such services (n.d.).

Terre des Hommes (English for *Land of People*) is a Swiss NGO that aims to protect children who have been victims of sexual abuse and to prevent the sexual abuse of children worldwide. The NGO operates by seeking CSAM forums on the Dark Web directly and engaging in conversations with offenders. By using artificial intelligence, the NGO created a lifelike avatar of a 10-year-old Filipino girl nicknamed "Sweetie", which would offer her services in certain dark web forums (Shobana et al., 2022). The character was present in the profile picture of the user in the forums, and the avatar was only responding if they received a message from some of the users (Chertoff & Jardine, 2021). After contacting Sweetie, the NGO activist who controlled Sweetie would ask the offenders to continue the conversation on Skype, where the identity and the location of offenders would be easier to uncover. The offenders would have to pay an amount to Sweetie to continue the conversation sexually through Skype, where the NGO captured their identities (S. & Randhawa, 2020). After capturing the identities, the NGO would perform an open-source investigation to uncover the key information of the offenders by cooperating with different law enforcement agencies (Rajamäki et al., 2022).

In 10 weeks, more than 20 thousand users contacted Sweetie and more than 800 offenders agreed to pay money to Sweetie to continue the conversation more intimately. Out of the offenders that contacted Sweetie, most of them were from the USA, the UK, and India. The operation and the arrests led to the bizarre conclusion that for just one account or child, there is a colossally large number of offenders and potential offenders who are willing to perform sexual acts or watch sexual acts with a minor (Raven et al., 2021). The operation led to international arrests of hundreds of individuals who agreed to sexual acts with Sweetie, and it showed how the approach can lead to sure convictions, with proactivity being the key in such investigations.

While Operation Sweetie cannot be classified in the above-mentioned 3-step modus operandi of dark web CSAM offenders, it shows how a different approach can lead to convictions quicker than after they already had occurred. It also shows how new approaches need and should be developed using all the aspects of available techniques. Furthermore, it highlights the importance of international cooperation between international law enforcement agencies. The large number of users and individuals interested in CSAM is alarming enough that a reactive approach is not going to be helpful or cover the true extent of such investigations. The people arrested and the offenders captured with Operation Sweetie were captured before they could do serious harm to a real child, which would cause more child victims in the world.

4.4 Discussion: Combating Child Abuse on the Dark Web

This chapter includes a short discussion of the previously presented literature review and the case studies, together with ideas on how to prevent and combat child abuse in the dark web.

Previous case studies and the literature revealed one fact that was visible and confirmed throughout the research—the problem of child abuse and its presence in the dark web is international, ever-present, and requires almost double the number of law enforcement agents than are currently employed in cyber investigations in all the Interpol countries combined, reaching millions of users worldwide daily (Van Der Bruggen & Blokland, 2021). Furthermore, the investigation is often hindered by the technological implications of the dark web, with the number of victims continuing to rise during the investigation itself. An additional constraint is that the offenders hosting such websites are often creating backup files, and compared to the Silk Road case, seizure, and shutdown of CSAM websites often lead to other websites being created at the same time, creating a continuous and never-ending cycle of the phenomenon of Child Abuse in the process (Van Der Bruggen & Blokland, 2021).

Confronted with such a vast number of potential cases and the permanent knowledge of the existence of CSAM materials on the dark web, the question is imposed as to how to combat child abuse on the dark web and improve the detection of child abusers before they can continue with their criminal behavior. Child Abuse causes long-term physical and psychological damage to the victims, their families, their parents, and even the investigators assigned to detect and find the offenders (Ngo et al., 2024). After the dark web became available, investigators learned the true extent of this phenomenon, and child abuse in the dark web became a global phenomenon.

Because the number of cases of child abuse in the dark web is increasing annually, and offenders can come from different backgrounds and different social environments, investigating and combating child abuse and CSAM facilitation in the dark web requires a complex multi-facetted approach that requires the cooperation of social services, international law enforcement agencies, interlinked investigative teams (e.g., family crimes working together with drug enforcement and child abuse online investigators), non-government organizations, online activists and free internet investigators to become successful. The three cases presented in this analysis show how different approaches and different investigative techniques were successful in capturing the offenders connected to the cases (Kloess & Van der Bruggen, 2023).

Compared to the Playpen and the Matthew Falder case, Operation Sweetie shows that it is required to change the approach to combating child sexual abuse on the dark web to prevent the number of victims from increasing and children from being harmed by such offenders. This would reduce the psychological strain on the investigators as well since counseling is required due to the graphic content investigators are presented in cases such as Matthew Falder and Playpen (Davis & Arrigo, 2021). However, this does not remove the necessity of tracking and observing the behavior of dark web CSAM users. Moreover, these two techniques should be combined

with classical law enforcement investigations and international cooperation to help combat the problem of child abuse material appearing on the dark web. Additionally, the fight needs to involve NGOs, social workers, and aid workers, and include social awareness campaigns, since the problem must be combated from different sides.

Reactive approaches show the disadvantage that there are most likely already victims at the time that the website was reported or discovered. Furthermore, investigative techniques and gathering of the key information take time, in which websites gain more users and probably present more victims. Law enforcement also needs to operate covertly on the dark web site and collect information and evidence, which also leads to victims continuing to suffer. Since the victims in such cases are children, the psychological impact on the investigators and prosecutors is implicit, which also constrains the ability of investigators and prosecutors to focus on the given task.

NGOs and online investigators have presented a more proactive or active approach, with NGOs creating online avatars and personas that interact directly with the offenders and provide information to law enforcement. Active investigators often approach individuals in online forums and bait them into a meeting where the offenders are being exposed and their information shared openly on the internet (Kokolaki et al., 2020). However, the disadvantage of active investigation by untrained individuals can result in dangerous situations during the confrontation and a significant threat to the investigators. Additionally, these approaches are often deemed unconstitutional and require active investigators to hand their evidence to the authorities. Investigations using AI to create online avatars have been shown to bear success, mainly because they actively engage with offenders and do not cause harm to the investigators or threaten their security. However, this approach must also undergo constant changes and adaptation to follow the changes in the modus operandi of the offenders posting CSAM on the dark web.

The social aspect and the interconnection of dark web child abuse cases require a multi-faceted approach. Offenders using the dark web to consume and share CSAM can also use the dark web to purchase drugs or run other illegal activities next to their main activity. It was revealed that child victims can come from different environments and the offenders can also be of different social status and different technological knowledge levels. Hence, social services must be made aware and observant of any particularities in the behavior of the subjects investigated, especially in impoverished and socially fragile areas. The latter is also indicated through the Matthew Falder case, where Falder and Scully aimed to abuse victims seeking help or offering services online, and Scully preyed on children in poor areas in the Philippines (Akhgar et al., 2021). A fruitful combination of investigative techniques combines proactive, reactive, and active approaches to the phenomenon of CSAM and child abuse in the dark web. Child abuse on the dark web is not likely to be exterminated any time soon, and the fight against it should become a complex international operation involving law enforcement agencies, NGOs, and online investigators, as well as awareness-raising campaigns to show how complex the problem is. Additionally, parents and caregivers should be made aware of how to protect their children and how to notice deviancy in behavior to avoid putting their children in dangerous situations (Davis & Arrigo, 2021).

5 Conclusions

Child abuse, regardless of whether of sexual nature or not, is one of the most horrifying criminal acts in existence. The problem of child sexual abuse has stunned criminal investigators for the severity and the people involved. While history has recorded different numbers of sexual abuse cases of children, the dark web turned this criminal phenomenon into a large-scale international problem. The dark web offers users of CSAM forums anonymity and protects their identities from law enforcement, giving the offenders a sense of security and assuring them that they are safe in their criminal behavior. The dark web also made CSAM accessible to anyone in the world who is sexually attracted to children and intends to explore its criminal attractions. Since the introduction of the dark web, the problem of CSAM shared on dark web forums exploded to the number of hundreds of millions of web pages with millions of users sharing, consuming, and trading CSAM. The problem becomes terrifying when thinking that each video, each picture, and each text is made by terrorizing a child and each object traded on dark web forums has a victim behind it.

To summarize: the problem of child abuse in the dark web overwhelms the number of available law enforcement capacities worldwide. This poses a significant problem that CSAM on the dark web is circulating, without the end being in sight. Law enforcement agencies employ different techniques to detect and capture offenders, with one technique being the creation of hacks that are posted on websites containing CSAM, like the Network Investigating Techniques, or the technique to register websites on dark web hosting platforms to get insights into the webpages and the activities on these to gather insights into the platforms and the users. Further investigation techniques include using artificial intelligence to create online avatars and catching sexual predators on CSAM dark web forums. All the techniques mentioned have their advantages and disadvantages. It is often too late when the CSAM forum has been discovered since by then there are already certain victims.

Child abuse on the dark web has a significant psychological and physical impact on the victims and their families. With the dark web providing such a large criminal extent to the phenomenon of child abuse, there are large threats of great international child abuse rings being created, that would operate in secrecy, and which could lead to a very large number of victims.

Due to the large extent of child abuse on the dark web and the international threats impacting all children worldwide, law enforcement agencies must rethink their approach to combating the problem. A multi-faceted approach could be a solution, which would require all law enforcement agencies to cooperate on a global level and share information about certain websites with alleged CSAM. Furthermore, the cooperation should include other social factors, such as NGOs and social workers. The approach should also be interconnected, including different agencies of law enforcement to verify if there are certain connections between CSAM and other criminal acts. Furthermore, law enforcement agencies must make use of artificial intelligence and create proactive and active approaches using AI avatars to directly approach offenders, detect their location, and apprehend them before they can cause

more harm. Additionally, the public and social services must launch awareness-raising campaigns to educate the public about the complexity of the problem. These campaigns should also include protection measures for parents, which would have a significant impact on the prevention of child abuse. Social welfare services should also be made aware of how to evaluate the parents since many cases have revealed that most victims living in economically stable conditions were abused by their parents. Social workers in impoverished areas and socially challenging areas should cooperate closely with law enforcement to prevent sex trafficking and sexual abuse in such areas since many cases revealed that children were lured by predators from challenging areas.

The implications for future research should result in the presentation of the multifaceted approach that includes all sorts of agencies and services combating the problem of child abuse in the dark web, and the further exploration of the proactive approach against CSAM using artificial intelligence. It also requires certain changes to the legal systems to prevent illegalities from arising in the prosecution of the offenders caught. Sadly, one cannot expect the problem of child abuse on the dark web to be finished soon, which is why parents must also be made aware of how they can protect their children, and authorities must be trained in how to protect the children from their parents. The problem of child abuse on the dark web will be a complex problem for law enforcement in the future and the focus for the future should be made on international cooperation, education, and coordination to protect children from becoming victims and stopping predators in the world who cause irreparable damage to children.

References

Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (2021). *Dark Web Investigation.* Cham: Springer.

Chertoff, M. (2023). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 26–38.

Chertoff, M., & Jardine, E. (2021). Policing the Dark Web: Legal Challenges in the 2015 Playpen Case. *GIGI Papers*, 1–24.

Chiang, E. (2024). Chiang, E. (2024). "I read the rules and know what is expected of me": The performance of competence and expertise in 'newbie'offenders' membership requests to dark web child abuse communities. *Discourse, Context & Media*, 100744.

Chopin, J., & Decary-Hetu, D. (2023). Dark web Pedophile Site Users' Cibersecurity Concerns: A lifespan and survival analysis. *Journal of Criminal Justice*, 86.

Dalins, J., Wilson, C., & Carman, M. (2022). Criminal Motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, 62–71.

Davis, S., & Arrigo, B. (2021). The Dark Web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change*, 367–386.

Demetis, D., & Kietzmann, J. (2021). Online child sexual exploitation: A new MIS Challenge. *Journal of the Association for Information Systems*, 9.

Fortin, F., & Paquette, S. (2022). Online sexual exploitation of children. *Sexual offending: A criminological perspective*, 237–256.

Gannon, C., Blokland, A., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. (2023). Child Sexual Material on the Internet. *International Journal of Innovative Forensic Psychiatry, Psychology, Criminology*, 353–365.

Guerra, E., & Westlake, B. G. (2023). Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites. *Child Abuse & Neglect 122*, 105336.

Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *Journal of Online Trust and Safety*, 1.

Jardine, E. (2022). The Dark Web Dilemma: Tor, anonymity, and online policing. *Global Commission on Internet Governance Paper Series*, 21.

Kloess, J. A., & Van der Bruggen, M. (2023). Trust and relationship development among users in Dark Web child sexual exploitation and abuse networks: a literature review from a psychological and criminological perspective. *Trauma, Violence, & Abuse*, 1220–1237.

Kokolaki, E., Daskalaki, E., Psaroudaki, K., Christodulaki, M., & Fragopolou, P. (2020). Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. *Computer Law & Security Review*, 38.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (2022). Child sexual abuse material online: the perspective of online investigators on training and support. *Policing: A Journal of Policy and Practice*, 762–776.

Ngo, V., Gajula, R., Thorpe, C., & Mckeever, S. (2024). Discovering child sexual abuse material creators' behaviors and preferences on the dark web. *Child Abuse & Neglect*, 106558.

Owens, J. N., Clapp, K., Craun, S. W., van der Bruggen, M., van Balen, I., van Bunningen, A., & Talens, P. (2023). Analysis of topic popularity within a child sexual exploitation Tor hidden service. *Aggression and violent behaviour*, 101808.

Rajamäki, J., Lahti, I., & Parviainen, J. (2022). Open Source Intelligence on the Dark Web: Child Abuse Material Investigations. *Information & Security*, 21–32.

Raven, A., Akhgar, B., & Abdel Samad, Y. (2021). Case Studies: Child Sexual Exploitation. In B. Akhgar, M. Gercke, S. Vrochidis, & H. Gibson, *Dark Web Investigation* (pp. 249-266). Cham: Springer.

S., K., & Randhawa, S. (2020). Dark Web: A web of crimes. *Wireless Personal Communications*, 2131–2158.

Shobana, A., Kaveri, R. N., Rethi, L., & Sajitha, K. (2022). Child Abuse Risk Prediction and Prevention Framework using AI and Dark Web. *International Journal of Innovative Analyses and Emerging Technology*, 51–57.

Van Der Bruggen, M., & Blokland, A. (2021). A crime script analysis of child sexual exploitation material fora on the darkweb. *Sexual Abuse*, 950–974.

van der Bruggen, M., & Blokland, A. (2021). Child sexual exploitation communities on the Darkweb: How organized are they. *Cybercrime in context: The human factor in victimization, offending, and policing*, 259–280.

van der Bruggen, M., & Blokland, A. (2022). Profiling Darkweb child sexual exploitation material from members using longitudal posting history data. *Social Science Computer Review*, 865–891.

Wang, Y., Arief, B., Franqueira, V. N., Coates, A., & Ciardha, C. (2023). Investigating the Availability of Child Sexual Abuse Materials in Dark Web Markets: Evidence Gathered and Lessons Learned. *European Interdisciplinary Cybersecurity Conference*, 59–64.

Westlake, B., & Guerra, E. (2023). Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the Dark Web. *Forensic science international: digital investigation*, 301620.

Blockchain Forensics & Public–Private Alliances: Tackling Child Exploitation on the Dark Web



Ahmad Alsuwaidi and Irenee Dondjio

1 Introduction

The dark web, an encrypted and hidden part of the internet, has become a hub for illegal activities, most alarmingly the distribution of child sexual abuse material (CSAM). Anonymity-enhancing technologies like The Onion Router (Tor) and cryptocurrencies enable perpetrators to evade detection (Kaur & Randhawa, 2020). Though the dark web comprises only a small fraction of the internet, its significant role in facilitating child exploitation presents an ongoing challenge for global law enforcement agencies (Spalevic & Ilic, 2017). It is estimated that as much as 80% of the dark web's activity is linked to CSAM, highlighting the urgency of developing effective countermeasures (Divakarmurthy et al., 2024).

A critical enabler of these crimes is cryptocurrency, which provides a level of anonymity that traditional financial systems cannot. Bitcoin was initially favored by criminals due to its decentralized nature, but its semi-transparent ledger has led many to adopt privacy-focused cryptocurrencies like Monero and Zcash (Shahzad et al., 2024). These privacy coins are designed to obscure transaction details, presenting significant hurdles for investigators. For instance, in a Brazilian Federal Police operation, over 6.2 million views of CSAM across 67 distinct categories were uncovered on a single dark web platform (Divakarmurthy et al., 2024). The scale of these crimes and the anonymity provided by cryptocurrencies underscore the need for advanced blockchain forensic techniques.

Despite advances in forensic technology, significant gaps remain. First, forensic tools tailored to tracing privacy-focused cryptocurrencies like Monero and Zcash are limited, posing a major hurdle in identifying the sources of illicit funds. Furthermore,

A. Alsuwaidi (✉)
Dubai Police Academy, Dubai, UAE
e-mail: adhahi@dubaipolice.ac.ae

A. Alsuwaidi · I. Dondjio
Nicosia University, Nicosia, Cyprus

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_3

the evolving tactics used by dark web criminals, including cryptomixing services and tumblers, further complicate investigation efforts. Another critical gap lies in the lack of efficient collaboration between public law enforcement agencies and private forensic firms. While some partnerships exist, there is a need for more structured frameworks to facilitate seamless information sharing and technological innovation. Additionally, global regulatory inconsistencies surrounding cryptocurrency use further hinder law enforcement's ability to intervene.

This chapter is structured as follows: it begins with an examination of the role of cryptocurrencies in facilitating child exploitation on the dark web, followed by a detailed analysis of forensic techniques and public–private collaborations. The paper then presents case studies of major law enforcement operations, addresses the challenges in cross-border cooperation, discusses technological advancements in blockchain forensics, and explores the need for global regulatory frameworks. Finally, it offers recommendations for future research, policy development, and strategies to enhance law enforcement capabilities and international collaboration in combating illicit activities.

2 Cryptocurrencies in Dark Web Child Exploitation

2.1 Bitcoin: Traceable yet Popular

Blockchain technology, known for its transparency, traceability, and data security, has been proposed to enhance the efficiency and reliability of cryptocurrencies (Dondjio & Themistocleous, 2021). However, despite its secure framework, certain cryptocurrencies, such as Bitcoin, are frequently used in illicit activities on the dark web, including child exploitation. While Bitcoin is often mistakenly believed to offer complete anonymity, each transaction is permanently recorded on its public blockchain. This transparency allows law enforcement and forensic experts to trace transactions, provided they have the necessary tools and expertise to analyze the data. By analyzing the blockchain, investigators can follow the movement of funds, identify associated wallets, and potentially uncover the identities behind these illicit activities (Raman et al., 2023).

While users are identified only by pseudonymous wallet addresses, law enforcement agencies can uncover real identities by linking transactions across exchanges or tracing payments to services that require identity verification. A notable example is Operation DisrupTor, where global authorities successfully traced Bitcoin transactions, resulting in 179 arrests worldwide and a seizure worth $6.5 million worth of cryptocurrencies (Europol, 2020). Despite these breakthroughs, Bitcoin remains a favored option on the dark web because of its widespread use and ease of access, presenting a paradox: its traceability does not deter criminals, perhaps because of its liquidity and familiarity (EUROPOL, 2021). Therefore, law enforcement agencies

are constantly advancing their blockchain forensic tools to keep pace with Bitcoin's continued popularity among illicit users.

2.2 *Monero and Zcash: Privacy Coins and Their Role in Obfuscation*

In contrast to Bitcoin's public ledger, privacy coins, such as Monero and Zcash, have grown in popularity among criminals because of their enhanced privacy. Monero employs techniques, such as ring signatures and stealth addresses, which effectively obscure the sender, recipient, and transaction amount, making it nearly impossible to trace through traditional blockchain analysis (Wei et al., 2024). Zcash takes privacy a step further by offering optional privacy protection through zk-SNARKs, a cryptographic method that allows transactions to be verified without revealing their details (Diro et al., 2024). These robust privacy features create significant hurdles for blockchain forensic experts because transactions involving Monero and Zcash are far more challenging to trace than those involving Bitcoin. In Operation Bayonet, for instance, authorities were limited in their ability to trace zero transactions because of inherent obfuscation mechanisms (Koerhuis et al., 2020). The growing use of privacy coins for dark web activities, particularly in illicit networks, underscores the increasing demand for advanced forensic tools and close collaboration between law enforcement and private forensic firms, as these technologies enhance anonymity and complicate transaction tracing (Childs, 2025).

2.3 *The Use of Cryptomixing Services to Hide Transactions*

Cryptomixing services, or "tumblers," are another key tool used by criminals to obscure their cryptocurrency transactions. These services pool multiple transactions together, scrambling the origin and destination of funds and making it nearly impossible to trace the flow of payments through standard blockchain analysis (Patsakis et al., 2023). In the case of child exploitation, cryptomixing services have been employed to conceal the movement of Bitcoin and other cryptocurrencies, making it exceedingly difficult for investigators to track payments to and from illicit platforms. One high-profile example is the AlphaBay marketplace, which relies heavily on cryptomixing services to conceal illegal financial activity (FBI, 2017). It is estimated that 30% of all Bitcoin transactions on the dark web involve some form of mixing service, which speaks to the scale of this challenge (Childs, 2025). Although blockchain forensic tools are evolving to counter these obfuscation techniques, cryptomixing remains a significant roadblock for law enforcement. Forensic experts are developing new methods that leverage pattern analysis and transaction clustering to

untangle the web created by these services. However, the battle between criminals and investigators remains ongoing (Hamilton & Leuprecht, 2024).

2.4 Key Challenges for Law Enforcement

The increasing prevalence of digital assets has demonstrated the transformative potential of blockchain technology. Its integration into digital asset ownership and transfer frameworks has significantly enhanced security, transparency, and efficiency in managing and transferring assets across various industries (Dondjio & Kazamias, 2023). However, the rapid rise of cryptocurrencies—especially privacy coins and cryptomixing services—has posed substantial challenges for law enforcement agencies attempting to combat child exploitation on the Dark Web. These privacy-focused tools enable criminals to obscure their financial activities, making it more difficult for authorities to trace and disrupt illicit transactions.

A key obstacle is the pseudonymous nature of cryptocurrency transactions, which obscures the identities of those involved. Unlike traditional financial systems, where personal information is often tied to transactions, cryptocurrency transactions are recorded on the blockchain without revealing the real-world identities of users. This makes it exceedingly difficult for investigators to trace and link illicit transactions to specific individuals unless they have access to additional data, such as records from cryptocurrency exchanges or cooperation from Internet service providers (Human Trafficking Front, 2023). Moreover, as criminals become more technologically savvy, they increasingly turn to decentralized exchanges (DEXs) such as Uniswap and Bisq, where they can trade cryptocurrencies without undergoing identity verification processes. These platforms operate without central oversight, allowing users to bypass the Know Your Customer (KYC) regulations that are typically required on centralized exchanges. This shift toward decentralized trading further complicates the ability of law enforcement to track and recover illicit funds, as the decentralized nature of these platforms makes it much harder to trace transactions or seize assets (Salisu & Filipov, 2023). As a result, law enforcement must continually adapt its strategies and tools to keep pace with the evolving tactics used by criminals in the digital age.

With the global cryptocurrency market reaching a capitalization of $1.03 trillion in 2021, it's clear that the stakes are high (Childs, 2025). Moreover, incidents like the $615 million Ethereum heist linked to North Korean hackers demonstrate the significant value of cryptocurrency transactions and the complex task of tracking stolen assets (Childs, 2025). Nevertheless, law enforcement agencies have had success, largely thanks to partnerships with private firms such as Chainalysis, whose tools have been instrumental in tracing Bitcoin and even some privacy coin transactions. Chainalysis' Reactor tool, for example, the Chainalysis Reactor tool has been used in several high-profile cases to trace criminal transactions across multiple blockchains (McShane, 2023). However, the rise of privacy coins and cryptomixing services demands constant innovation in forensic techniques, and emphasizes the

need for stronger partnerships between law enforcement and the private industry to stay ahead of these evolving challenges. The future of combating child exploitation on the dark web will depend not only on keeping pace with technological advancements but also on anticipating new tactics employed by criminals before they can become widespread.

3 Blockchain Forensics: Techniques and Tools

3.1 Address Clustering for Identifying Wallets

Address clustering is one of the most powerful techniques in blockchain forensics, frequently used to identify and group multiple cryptocurrency addresses that are likely controlled by a single individual or entity. This method plays a critical role in unraveling the often complex and fragmented nature of blockchain transactions. When cryptocurrencies like Bitcoin are used, each transaction can involve multiple input and output addresses, which can initially create a confusing web of connections that obscures the identity of the user behind them (Fröwis et al., 2020).

However, forensic tools are designed to cut through this complexity by analyzing transactional patterns and identifying links between addresses. One of the key patterns forensic investigators look for is the use of multiple input addresses in a single transaction. When a transaction draws from several input addresses, it is a strong indication that these addresses belong to the same wallet, as they all must collectively sign off on the transaction. By detecting such patterns, address clustering helps investigators group these addresses and associate them with a single wallet or user, revealing a clearer picture of the user's financial activities.

This technique becomes particularly valuable when individuals attempt to hide their tracks by fragmenting their transactions across multiple addresses, a common tactic used in illegal activities such as money laundering or dark web transactions. By clustering these fragmented addresses together, law enforcement can effectively trace the flow of funds across the blockchain, even when criminals try to scatter their digital footprint. As a result, address clustering allows investigators to overcome one of the key challenges in blockchain forensics: tracking and linking seemingly unrelated transactions back to a single entity (Qin et al., 2022). This technique has proven indispensable in forensic investigations, enabling law enforcement to trace illicit activities more efficiently and hold individuals accountable.

Building on the power of address clustering to link seemingly unrelated transactions, this technique has been instrumental in breaking through the anonymity of dark web users engaged in child exploitation who frequently rely on cryptocurrency transactions to purchase illegal content. Many criminals fail to fully obscure their wallet identities, often because of the complexity of keeping transactions anonymous. Forensic tools use clustering to build the profiles of these users, leading to their identification when wallet addresses can be linked to real-world data such as

transactions made through exchanges that require identity verification. In Operation DisrupTor, address clustering helped identify over 270,000 individual Bitcoin wallet addresses tied to dark web activity, contributing to 179 arrests and a seizure of $6.5 million in cryptocurrencies (Europol, 2020). These successes underscore the critical role of address clustering in unveiling hidden networks of child exploitation on the Dark Web (ICMEC, 2021).

3.2 Transaction Graph Analysis for Mapping Networks

Address clustering is not the only method crucial to blockchain forensics; another powerful technique is transaction graph analysis, which offers a visual and data-driven representation of cryptocurrency flows. This method involves creating a graph where nodes represent wallet addresses and edges represent the transactions between them, forming a map that reflects the movement of funds. Transaction graph analysis allows investigators to uncover patterns that may indicate illegal activities such as high volumes of transactions between suspicious addresses or repeated transfers that resemble money laundering schemes (Tharani et al., 2021).

This analytical method is particularly effective in tracing the networks of criminals involved in child exploitation on the Dark Web. Many dark web operators rely on a network of intermediaries to obfuscate the flow of payments, using layers of transactions and multiple addresses to disguise their tracks. Transaction graph analysis can reveal these layers by identifying indirect connections and transaction loops that may otherwise go unnoticed. For example, if multiple addresses continually exchange cryptocurrencies or repeatedly connect to key addresses, forensic analysts can flag them for further investigation. In AlphaBay takedown, law enforcement mapped over $23 million in cryptocurrency transactions, tracing these flows across multiple dark web platforms, and leading to the dismantling of significant criminal networks (FBI, 2017). Additionally, transaction graphs help identify not only the users making illegal purchases but also the service providers facilitating these transactions. Cryptocurrency exchanges and payment processors frequently interacting with suspicious addresses are of particular interest to law enforcement, as they may hold critical KYC (Know Your Customer) data. Machine learning algorithms are increasingly being used to enhance this process, allowing for more efficient identification of suspicious patterns in large datasets (Nicholls et al., 2024).

3.3 Network Analysis with Extended Safe Petri Net

Building upon transaction graph analysis, network analysis using the Extended Safe Petri Net (ESPN) provides a more advanced framework for modeling the complex interactions and behaviors within blockchain networks. While regular transaction

graph analysis is powerful, ESPN adds another layer by allowing analysts to incorporate behaviors and time-bound transactions into the network model. This results in a more dynamic and flexible view of cryptocurrency flows, particularly in the context of illegal networks (Pinna et al., 2018).

For example, an ESPN can represent transactions involving different cryptocurrencies, making it especially valuable in investigations where criminals use privacy-enhancing cryptocurrencies, such as Monero or Zcash, alongside more transparent ones, such as Bitcoin. The ESPN is also useful for modeling interactions with mixing services, which further complicates the tracing process. By simulating how these services interact with a broader blockchain, forensic experts can pinpoint key transition points where privacy is compromised or detect abnormal behaviors that indicate illicit activity (Silfversten et al., 2020). This approach was particularly valuable in Operation Bayonet, where ESPN was used to track complex cryptocurrency flows across multiple platforms. By understanding these flows in greater detail, law enforcement agencies can identify weaknesses in criminal operations and target them effectively. The ESPN model also visualizes transitions across different layers of the blockchain, such as side chains or off-chain solutions such as lightning networks, making it especially useful in investigations involving sophisticated criminal networks (Dasaklis & Malamas, 2023).

3.4 Multi-Layer Bitcoin Address Clustering for Dark Web Marketplaces

Expanding on traditional address clustering, multi-layer Bitcoin address clustering offers a more comprehensive approach by integrating additional data such as behavioral patterns, transaction metadata, and temporal analysis. This method provides investigators with a deeper understanding of the complex interactions within dark web marketplaces, where users, vendors, and marketplace operators engage in vast transactional ecosystems (Meiklejohn et al., 2016).

By layering this data, forensic analysts can go beyond merely identifying clusters of addresses controlled by a single user. Instead, they can uncover intricate relationships between different entities on the platform, mapping out how users interact with vendors and how transactions flow through the marketplace. This multi-dimensional approach enables law enforcement to pinpoint key actors within criminal networks, such as marketplace operators and prolific vendors, and track their movements across various blockchain layers (Kim et al., 2022).

Dark web marketplaces that facilitate child exploitation transactions often employ sophisticated payment systems designed to obfuscate sources and destinations of funds. However, multi-layer address clustering can identify patterns that reveal user behaviors, such as withdrawal timing, repeated interactions between certain wallet addresses, and the use of cryptomixing services. When analyzed over time, these patterns can be used to profile the most active participants, helping law enforcement

track down key operators and buyers. In Operation DisrupTor, multi-layer clustering allows forensic analysts to trace cryptocurrency flows across multiple marketplaces, identify overlapping users, and expose criminal networks operating on different platforms (Europol, 2020). By layering additional data points, such as the IP addresses of servers hosting dark web content or transaction timestamps, multi-layer clustering has enabled law enforcement to dismantle entire dark web ecosystems focused on child exploitation.

4 Case Studies

The following section will examine three pivotal case studies—DisrupTor, AlphaBay, and Welcome to Video—that showcase the effective use of blockchain forensic techniques in combatting child exploitation on the dark web. These cases were selected for their relevance, precision, and significant impact in dismantling large-scale illegal networks. Each highlights how law enforcement agencies, working closely with private forensic firms, utilized advanced cryptocurrency tracing tools to overcome the challenges of anonymity inherent in cryptocurrency transactions. The forensic methods employed, such as tracing through coin-mixing services and privacy coins, enabled the identification of key criminals and led to substantial arrests and cryptocurrency seizures. These outcomes underscore the importance of public–private partnerships in achieving tangible results in the fight against dark web child exploitation.

5 Case Study 1: Operation DisrupTor (2020)

5.1 Overview of the Operation and Its Focus on Child Exploitation

Operation DisrupTor, launched in September 2020, was a global law enforcement initiative led by the United States Department of Justice (DOJ) and Europol. While the operation targeted various illicit activities on the dark web, such as drug trafficking, it also focused heavily on disrupting child exploitation networks. Leveraging the infrastructure of earlier operations like Operation Bayonet (which targeted AlphaBay), DisrupTor aimed to dismantle criminal networks utilizing darknet platforms to distribute illegal content, including child sexual abuse material (CSAM). The operation resulted in 179 arrests worldwide, the seizure of over $6.5 million in cash and cryptocurrencies, and the removal of numerous darknet platforms used to facilitate these crimes (U.S. Department of Justice, 2020) (Fig. 1).

These arrests and seizures represent significant progress in combating child exploitation on the dark web. Darknet platforms often rely on cryptocurrencies like



Fig. 1 Operation DisrupTor Results. *Source* U.S. Department of Justice

Bitcoin and Monero to enable anonymous transactions, complicating law enforcement efforts. However, through close international cooperation with agencies such as the FBI, DEA, Homeland Security Investigations (HSI), Europol, and counterparts from Germany, the Netherlands, and the UK, Operation DisrupTor succeeded in targeting these criminal activities, marking a pivotal moment in disrupting the global ecosystem of online child exploitation (Europol, 2024).

5.2 Blockchain Forensic Techniques Used

The success of Operation DisrupTor was largely due to the deployment of advanced blockchain forensic tools designed to trace cryptocurrency transactions used in illicit activities. Tools such as Chainalysis, Elliptic, and CipherTrace were instrumental in helping law enforcement agencies track and analyze transactions on public blockchains like Bitcoin (Salisu & Filipov, 2023).

Key Blockchain Forensic Techniques Employed Included:

- **Address Clustering**: This technique helped group multiple blockchain addresses controlled by the same entity, enabling investigators to trace transactions across different darknet platforms. By identifying patterns across addresses, law enforcement could link transactions to specific vendors distributing child exploitation material. For example, during Operation DisrupTor, address clustering helped identify darknet vendors involved in illegal transactions across various platforms (De Lucci et al., 2024).

- **Transaction Graph Analysis**: Investigators used transaction graph analysis to map the flow of funds between wallets, which helped identify suspicious patterns, such as repeated use of obfuscation tactics or multi-hop transactions. This method enabled law enforcement to uncover complex networks of transactions, providing valuable insights into the flow of illicit funds. For instance, in Operation DisrupTor, this technique revealed hidden connections between wallets and the dark web's child exploitation networks (Wu et al., 2021).
- **Know Your Customer (KYC) Data**: KYC data from cryptocurrency exchanges proved crucial in linking anonymous blockchain wallets to real-world individuals. By collaborating with exchanges like Coinbase and Binance, law enforcement accessed identity verification data, which allowed them to trace flagged transactions back to the perpetrators. This collaborative effort between private exchanges and law enforcement was a key factor in unmasking those involved in child exploitation (Barbereau & Bodó, 2023).

These forensic techniques, particularly the use of address clustering and KYC data, were vital to the operation's success in disrupting the criminal networks responsible for child exploitation on the dark web.

5.3 Challenges in Tracing Monero Transactions

Monero, a privacy-focused cryptocurrency, presented significant challenges for law enforcement during Operation DisrupTor. Unlike Bitcoin, Monero uses advanced privacy features such as ring signatures, stealth addresses, and confidential transactions, which obscure transaction details like the sender, recipient, and amount. These features make Monero transactions nearly impossible to trace using traditional blockchain forensic tools (Möser et al., 2018).

Monero was a preferred cryptocurrency for darknet users due to its robust anonymity features, and its limited integration with mainstream exchanges further complicated efforts to track these transactions. Unlike Bitcoin, which is traded on numerous exchanges with strict KYC regulations, Monero's decentralized and private nature makes it particularly attractive to criminals. The lack of cooperation from exchanges dealing with Monero added another layer of complexity for investigators (Hamilton & Leuprecht, 2024). As a result, while Operation DisrupTor had success tracing Bitcoin transactions, the ability to track Monero remained limited, highlighting the ongoing challenges in dealing with privacy coins.

5.4 Impact and Outcomes: Dismantling Child Exploitation Networks

Operation DisrupTor was a major success in dismantling child exploitation networks on the dark web. Through the infiltration of darknet marketplaces, law enforcement seized platforms distributing illegal child exploitation material and arrested key individuals involved in these networks.

Key Outcomes Include:

- **Arrests and Convictions**: Numerous individuals involved in child exploitation networks were arrested, including key darknet administrators and vendors. These arrests significantly disrupted the distribution of child exploitation material by removing key figures responsible for managing these platforms (FBI, 2020).
- **Disruption of Darknet Infrastructure**: The operation's success in dismantling several darknet platforms hosting illegal content was critical. By removing these platforms, Operation DisrupTor effectively disrupted the infrastructure that facilitated the distribution of CSAM, severing access to thousands of users engaged in these illegal activities (FBI, 2020).
- **International Cooperation**: Operation DisrupTor showcased the importance of global collaboration, with law enforcement agencies from countries such as Germany, the UK, and the Netherlands working closely with US authorities. This international cooperation, including intelligence sharing and joint operations, played a crucial role in the operation's success (UNODC & WACAP, 2020).

While the operation marked significant progress, challenges remain—particularly with the growing use of privacy coins like Monero. However, the increased scrutiny on cryptocurrency exchanges and advancements in blockchain forensics represent positive steps forward in combating child exploitation on the dark web. The operation's impact continues to resonate, driving law enforcement to develop more sophisticated forensic tools and foster stronger partnerships with the private sector to address these evolving threats (U.S. Department of Justice, 2020).

6 Case Study 2: Operation Bayonet and the AlphaBay Takedown

6.1 Overview of AlphaBay's Role in Child Exploitation

Before its takedown in July 2017, AlphaBay was the largest darknet marketplace, facilitating a wide range of illicit activities, including the distribution of child sexual abuse material (CSAM). AlphaBay operated on the Tor network, which provided users with anonymity while conducting illegal transactions using cryptocurrencies like Bitcoin, Ethereum, and Monero (Department of Justice, 2017). Although the

primary focus of the platform was drug trafficking, sections dedicated to adult content, including child exploitation material, became a major part of its operations. Vendors used the platform to sell CSAM, with the use of cryptocurrencies ensuring a level of anonymity that complicated law enforcement efforts to trace illegal activities (Europol, 2017).

Child exploitation networks leveraged AlphaBay's vast and anonymous infrastructure to traffic illegal content globally. The anonymous nature of transactions, coupled with privacy coins like Monero, created a haven for criminals. The absence of direct oversight allowed the platform to operate with impunity, posing an enormous challenge to law enforcement agencies tasked with tracking down the individuals behind these crimes (Leonid & Vladimir, 2023). The scale of the operation, combined with the difficulties of tracing cryptocurrency transactions, required the use of advanced forensic tools and international cooperation.

6.2 Bitcoin and Ethereum Tracing: Tools and Techniques

The takedown of AlphaBay marked one of the most significant successes in combating illegal activities on the dark web. Blockchain forensic tools played a pivotal role in tracing Bitcoin and Ethereum transactions, the two most used cryptocurrencies on the platform. Law enforcement used tools like Chainalysis, Elliptic, and transaction graph analysis to follow the flow of funds between wallets, uncovering links between anonymous addresses and real-world identities.

Address clustering was instrumental in this process, grouping multiple wallet addresses under a single entity to map the flow of cryptocurrency through the dark web (Qin et al., 2022). Law enforcement agencies were able to track illicit funds through exchanges and identify individuals involved in illegal activities, such as those dealing in CSAM. Taint analysis, which tracks cryptocurrency transactions associated with criminal activity, further helped trace Bitcoin and Ethereum as they moved through the AlphaBay network (Leonid & Vladimir, 2023).

By collaborating with cryptocurrency exchanges that implement Know Your Customer (KYC) protocols, such as Coinbase and Kraken, law enforcement obtained critical data linking wallet addresses to real-world identities. This cooperation between exchanges and authorities was crucial in the identification and apprehension of criminals involved in AlphaBay's illegal activities (Ncube & Kabwe, 2023).

6.3 Privacy Coins in AlphaBay: The Role of Monero

While Bitcoin and Ethereum were traceable, privacy coins like Monero posed a significant challenge for law enforcement. Monero's enhanced privacy features, including ring signatures, stealth addresses, and confidential transactions, were specifically designed to protect the identities of senders and receivers and obscure

transaction amounts (Wijaya et al., 2019). These features allowed AlphaBay users engaged in child exploitation to evade detection, complicating efforts to track funds.

Monero's popularity on AlphaBay stemmed from its ability to offer near-total anonymity, making it extremely difficult for traditional blockchain forensic tools to trace transactions. However, law enforcement adapted by analyzing patterns in user behavior and tracking conversions from Monero to traceable cryptocurrencies like Bitcoin and Ethereum. In some cases, vendors had to exchange Monero for Bitcoin to access certain services or liquidate their holdings, offering investigators a potential avenue for tracing illicit transactions across multiple currencies (Hamilton & Leuprecht, 2024).

6.4 Outcomes of Operation Bayonet: Arrests and Seizures

Operation Bayonet, a collaborative effort involving the FBI, DEA, Europol, and other international law enforcement agencies, culminated in the global takedown of AlphaBay in July 2017. The operation resulted in several critical outcomes, including the arrest of AlphaBay's founder, Alexandre Cazes, in Thailand, and the seizure of millions of dollars in cryptocurrencies, including Bitcoin, Ethereum, and Monero (US Attorney's Office, 2024).

Beyond the arrest of AlphaBay's leadership, Operation Bayonet led to the identification and apprehension of key vendors involved in CSAM distribution. This dismantling of AlphaBay's infrastructure also led to a significant disruption of darknet operations, forcing many users and vendors to migrate to smaller platforms, none of which achieved the same scale or security. The operation increased global scrutiny on dark web markets and led to intensified law enforcement efforts targeting cryptocurrency exchanges facilitating illegal transactions (Department of Justice, 2017).

The success of Operation Bayonet underscored the critical role of blockchain forensics in dismantling dark web networks and highlighted the importance of public–private partnerships. Cooperation between law enforcement agencies and private forensic firms like Chainalysis and Elliptic was key in tracking cryptocurrency transactions and linking anonymous users to real-world identities. Although challenges remain, particularly in tracing privacy coins like Monero, Operation Bayonet marked a turning point in the fight against child exploitation and other illicit activities on the dark web.

6.5 Lessons Learned and Future Outlook

Operation Bayonet highlighted several key lessons for future efforts to combat child exploitation on the dark web. First, the importance of international cooperation cannot be overstated. The collaboration between law enforcement agencies across multiple countries, as well as with private sector forensic firms, played a pivotal role

in AlphaBay's takedown. Second, the operation showcased the evolving nature of blockchain forensics, with investigators having to continuously adapt to new privacy technologies like Monero.

Moving forward, law enforcement agencies will need to develop even more advanced forensic tools and strategies to address the growing use of privacy-enhancing cryptocurrencies and obfuscation services on the dark web. The success of Operation Bayonet demonstrates that while challenges remain, public–private partnerships and cutting-edge forensic technologies can significantly impact the fight against child exploitation and other illegal activities on the dark web.

7 Case Study 3: The "Welcome to Video" Investigation

7.1 The Dark Web's Largest Child Exploitation Takedown

The "Welcome to Video" investigation is one of the most significant child exploitation takedowns in dark web history. Launched in 2015, the illicit website operated by the South Korean national Jong Woo Son became a hub for the distribution of child sexual abuse material (CSAM). Over the course of its operation, the platform amassed over 250,000 unique videos and facilitated more than 1 million downloads of CSAM downloads. This site catered to a global network of predators, with users paying for access to this material using Bitcoin, which was selected for its perceived anonymity. Through Bitcoin transactions and the Tor network, users believe that they could remain anonymous while committing these heinous acts (Celiksoy et al., 2023).

The scale of the "Welcome to Video" platform attracted the attention of international law enforcement agencies, who began pooling resources to investigate and dismantle the network. The site's takedown in 2019 marked a pivotal moment in the global fight against online child exploitation, revealing the immense scale of dark web child abuse networks and the vulnerabilities even in highly anonymized systems (Holt et al., 2022).

7.2 Blockchain Forensic Methods Used to Trace Bitcoin Transactions

The "Welcome to Video" investigation's success was largely due to blockchain forensic methods, which enabled law enforcement to trace Bitcoin transactions linked to the platform. Agencies such as the Internal Revenue Service—Criminal Investigation (IRS-CI) and Homeland Security Investigations (HSI) use tools such as Chainalysis and CipherTrace to track Bitcoin's public ledger, analyze clusters of transactions, and follow the flow of funds from one wallet to another. These forensic

techniques allow investigators to map the networks of users who believe they are operating anonymously (Salisu & Filipov, 2023).

Blockchain's immutable nature, in which every transaction is permanently recorded, is key to law enforcement's ability to uncover patterns between wallets. The analysis was particularly effective when users made the mistake of purchasing Bitcoin through exchanges that required Know Your Customer (KYC) protocols, allowing authorities to connect Bitcoin wallets to personal identities. These data points, when combined with traditional investigative methods, enable law enforcement to expose vast networks of individuals involved in CSAM (Nicholls et al., 2024).

In addition to tracking transactions within the Bitcoin ecosystem, investigators have focused on the conversion of illicit cryptocurrencies into fiat currencies. By following the digital breadcrumbs left behind, they were able to identify users who believed their transactions could not be traced back. This further demonstrates the effectiveness of blockchain analytics in breaking through the layers of anonymity that dark web users rely on (Salisu & Filipov, 2023).

7.3 Operational Mistakes and Law Enforcement Breakthroughs

Despite operating on the dark web, "Welcome to Video" administrators made several critical errors that ultimately led to their downfall. One of the most glaring mistakes was their reliance on Bitcoin for transactions. Unlike privacy-focused cryptocurrencies such as Monero, Bitcoin is pseudonymous but not fully anonymous, meaning that its transactions are recorded on a transparent blockchain. The site's administrators also failed to properly anonymize Bitcoin addresses, recycle the same addresses for multiple transactions, and make it easier for law enforcement to trace illicit funds (UNODC, 2022).

In addition, the platform's servers were hosted in South Korea, which, despite being hidden behind Tor's anonymizing network, left clues that could be traced through law enforcement. Investigators were able to follow digital breadcrumbs to physical servers, thereby gaining critical information about the platform's operations, users, and administrators. The poor operational security of administrators provided key openings that investigators could exploit, proving that even on the dark web, mistakes can compromise security (UNODC, 2022).

7.4 Global Impact: Arrests and Rescue Operations

The takedown of "Welcome to Video" had a significant global impact, leading to the arrest of over 337 individuals across 38 countries. These arrests included child

predators, individuals involved in uploading videos, and those participating in the CSAM exchanges. In addition to the arrests, 23 children were rescued from direct abuse, many of whom were victims filmed for videos distributed on the platform (U.S. House Committee on Financial Services Democrats, 2024).

International cooperation is pivotal for achieving these outcomes. Agencies such as Interpol, Europol, and the United Kingdom's National Crime Agency (NCA) worked closely with US authorities to track offenders across multiple jurisdictions. The investigation underscored the necessity of global collaboration in combating child exploitation, where criminals often operate across borders and take advantage of the global nature of the internet. Figure 2 illustrates the banner displayed after the site was seized by international law enforcement agencies, symbolizing the success of global collaboration in dismantling the platform.

The takedown of "Welcome to Video" sent shockwaves through dark web communities, particularly those involved in CSAM, signaling that the reach of law enforcement extends even to the deepest corners of the Internet. This operation was widely hailed as a success in leveraging blockchain forensics and international partnerships to dismantle one of the most prolific CSAM networks in the history (Raman & Shults, 2020).



Fig. 2 "Welcome to Video" website seized banner. *Source* Welcome to Video website

8 Public–Private Partnerships in Cryptocurrency Tracing

Cryptocurrency tracing is a domain where public and private entities collaborate. Governments, law enforcement agencies, and private blockchain forensic firms work together to combat cybercrime, money laundering, and financing child exploitation (Hamilton & Leuprecht, 2024). This section explores the importance of these partnerships and evaluates their role in successful operations against illicit activities on the Dark Web.

8.1 Role of Blockchain Forensics Firms in Supporting Law Enforcement

Blockchain forensic firms, such as Chainalysis, CipherTrace, and Elliptic, have become essential partners in law enforcement efforts to trace illicit cryptocurrency transactions. These firms provide advanced tools, technologies, and expertise, beyond the capabilities of traditional law enforcement agencies. Blockchain analytics can map the flow of digital assets, identify patterns of suspicious transactions, and link cryptocurrency wallets to real-world identities (McShane, 2023).

Forensic firms support law enforcement by offering specialized investigative tools, training programs, and real-time monitoring services. Tools such as Chainalysis Reactor and Elliptic Navigator provide visual representations of blockchain transactions, enabling law enforcement agencies to trace the movement of funds and pinpoint criminal actors. Forensic firms also offer training workshops to help law enforcement agencies build their internal expertise in blockchain investigation. By utilizing real-time analytics, private firms can monitor fund movement, allowing law enforcement to act swiftly against emerging threats. These partnerships are crucial for overcoming technical barriers and enhancing the efficiency of investigations of dark web activities (Reedy, 2023).

8.2 Case Study Support: DisrupTor, AlphaBay, and Welcome to Video

The following section will delve into the outcomes of Operation DisrupTor, AlphaBay, and "Welcome to Video," showcasing how these collaborative efforts between law enforcement and blockchain forensic firms led to significant breakthroughs in dismantling child exploitation networks.

The success of public–private partnerships in cryptocurrency tracing can be seen in major dark web takedowns such as Operation DisrupTor, AlphaBay, and "Welcome to Video." Blockchain forensic firms play an integral role in providing the technology and expertise necessary for tracing cryptocurrency transactions tied to

these operations. During Operation DisrupTor, forensic firms help trace transactions across multiple cryptocurrencies, including those obscured by coin-mixing services designed to hide origins (Bahamazava & Nanda, 2022).

In the AlphaBay case, firms worked closely with law enforcement to trace Bitcoin and Ethereum transactions, offering vital insights into the marketplace's financial workings of the marketplace (Him, 2024). The takedown of "Welcome to Video," one of the largest child exploitation sites on the dark web, relied heavily on the precision of blockchain forensics in tracking Bitcoin payments used to purchase illegal content. Accurate tracking is key to arresting platform operators and rescuing victims (Nazah et al., 2020). These case studies underscore the pivotal role of private blockchain forensic firms in supporting law enforcement efforts, enabling the successful tracing of cryptocurrency transactions, even across privacy-focused platforms.

8.3 Addressing Challenges in Public–Private Collaboration

8.3.1 Lessons Learned

- **Data Privacy Concerns**: One of the significant challenges of public–private partnerships in cryptocurrency tracing is the large amounts of transactional data accessible to private firms. This raises serious concerns about privacy, as this data includes sensitive information. It is critical to balance the needs of security and law enforcement with the protection of individual privacy rights, which requires careful legal and ethical considerations (Uzougbo et al., 2024).
- **Jurisdictional Issues**: Cryptocurrency transactions frequently cross international borders, leading to jurisdictional challenges. The variations in legal frameworks across different countries make it difficult for law enforcement to enforce laws consistently. These differences can lead to delays in investigations and create obstacles for seamless cooperation across borders (Uzougbo et al., 2024).
- **Resource Allocation**: Many law enforcement agencies struggle with limited resources, making it difficult for them to fully utilize blockchain forensic tools. The high costs associated with these specialized services strain public budgets, and the lack of trained personnel further hinders the ability of agencies to effectively leverage blockchain forensic technologies (Shiva et al., 2023).
- **Coordination and Communication**: Effective collaboration between public and private entities is often hindered by poor communication. Misaligned goals or differing methodologies between public agencies and private firms can reduce the efficiency of joint operations. Seamless communication and well-coordinated strategies are critical for overcoming this challenge (Uzougbo et al., 2024).

8.3.2 Key Strategies

- **Improving Data-Sharing Protocols**: To address privacy concerns and improve collaboration, transparent and secure data-sharing protocols must be implemented between public agencies and private firms. Clear guidelines on how data is handled and shared will foster trust and facilitate more effective investigations (Shiva et al., 2023).
- **Harmonizing Legal Frameworks Across Borders**: Given that cryptocurrency crimes often involve cross-border transactions, there is a need for harmonized legal frameworks across jurisdictions. Aligning legal standards would reduce delays and complications caused by conflicting regulations, enabling law enforcement agencies to cooperate more effectively in international investigations (Uzougbo et al., 2024).
- **Investing in Resources for Law Enforcement**: Governments should allocate additional resources to law enforcement agencies to enable them to better leverage blockchain forensic services. This includes funding for the acquisition of specialized forensic tools and training personnel in blockchain analytics, ensuring that agencies have the capacity to manage complex investigations (Shiva et al., 2023).

8.3.3 Actionable Recommendations

- **Address Data Privacy Issues**: Governments and private firms should work together to create robust legal frameworks that ensure the responsible use of data, while safeguarding individuals' privacy. This will allow law enforcement to access necessary data without infringing on privacy rights, creating a more balanced approach to security (Uzougbo et al., 2024).
- **Standardize Cross-Border Investigations**: International collaboration can be improved by developing standardized procedures for handling cryptocurrency tracing across jurisdictions. Governments should work on creating legal frameworks that enable smooth cross-border collaboration, reducing delays caused by jurisdictional differences (Uzougbo et al., 2024).
- **Increase Investment in Blockchain Tools and Training**: Law enforcement agencies need to increase investments in blockchain forensic tools and the training of personnel. This will allow agencies to better manage cryptocurrency-related investigations without over-relying on external firms, ultimately improving the overall capacity to respond to cybercrime (Shiva et al., 2023).

9 Technological Advancements in Blockchain Forensics

Blockchain forensics has evolved substantially in recent years, driven by the growing need to counter illicit activities conducted through cryptocurrencies. The integration of technologies like artificial intelligence (AI), machine learning (ML), and enhanced tools for privacy coins such as Monero and Zcash, as well as real-time monitoring solutions, has reshaped how investigations are conducted. These advancements have enhanced law enforcement's capacity to tackle complex financial crimes, including money laundering, cyber fraud, and child exploitation (Japinye, 2024; Koerhuis et al., 2020).

9.1 AI and Machine Learning for Enhanced Transaction Detection

9.1.1 Lessons Learned

- **Efficiency in Detection**: AI and machine learning (ML) have revolutionized blockchain forensics by providing faster, more accurate detection of suspicious transactions. Traditional manual analysis is being replaced by AI-powered tools, which can process large volumes of blockchain data quickly. These tools can identify complex schemes like chain-hopping, where criminals move assets across multiple blockchains, and transaction stratification, where large sums of cryptocurrency are divided into smaller amounts to evade scrutiny (Tuli & Thaduri, 2023).
- **Behavioral Profiling of Wallets**: One of the major benefits of AI and ML in forensics is the ability to construct behavioral profiles of suspicious wallets. AI can detect unusual activities such as the use of mixers or tumblers that obfuscate transaction origins. Machine learning models also adapt to criminal tactics in real-time, continuously improving their ability to detect evolving criminal behaviors (George, 2023).

9.1.2 Key Strategies

- **AI for Real-Time Monitoring**: AI models have been instrumental in helping investigators detect and predict irregular activities across blockchain networks. AI tools allow for the real-time monitoring of multiple blockchains, flagging emergent threats and suspicious transaction clusters that could be missed through manual scrutiny (Dunsin et al., 2024).
- **Predictive Capabilities**: Predictive analytics, powered by machine learning algorithms, enables forensic experts to anticipate criminal activities by analyzing historical transaction data. These models can flag potential threats before they

escalate, helping authorities prevent crimes such as money laundering or child exploitation (McShane, 2023).

9.1.3 Actionable Recommendations

- **Enhance AI Integration**: Investment in AI and ML should continue, focusing on the development of more sophisticated tools that can detect increasingly complex criminal behaviors. AI tools should be capable of identifying new mixing services, detecting unusual transaction flows, and continuously learning from new data (George, 2023).
- **Real-Time Monitoring Expansion**: Real-time monitoring capabilities should be expanded to cover a broader range of blockchains. This will enable law enforcement to intervene faster, particularly in scenarios where funds may be moved quickly across different platforms or converted into fiat currencies (Dunsin et al., 2024).

9.2 Forensic Tools for Privacy Coins: Monero and Zcash

9.2.1 Lessons Learned

- **Anonymity Challenges**: Privacy coins like Monero and Zcash present significant obstacles for blockchain forensics due to their enhanced focus on anonymity. These coins were designed to shield transaction details from public scrutiny, making them attractive to criminals operating on the dark web (Koerhuis et al., 2020).
- **Monero's Privacy Features**: Monero uses advanced privacy features, including ring signatures, stealth addresses, and confidential transactions, all of which obscure the true sender, recipient, and amount involved in a transaction. This makes tracing these transactions highly difficult (Koerhuis et al., 2020).
- **Zcash's Dual-Transaction System**: Zcash offers both shielded (private) and unshielded (transparent) transactions, with the shielded ones fully obscuring transaction details. Forensic experts face challenges in tracking funds that move between these states, especially when they transition from shielded transactions into fiat currencies (Zhang et al., 2024).

9.2.2 Key Strategies

- **Developing Advanced Analytical Techniques**: For Monero, forensic experts are beginning to employ techniques like timing attacks, which analyze the timing of transactions to infer possible links between wallets. Metadata analysis, which focuses on scrutinizing off-chain data like node behavior and transaction timings,

also shows promise in penetrating the anonymity of privacy coins (Zhang et al., 2024).
- **Tracing Zcash Transactions**: By analyzing patterns in unshielded transactions and tracking the transition between shielded and unshielded states, forensic investigators can identify suspicious activities. This helps in cases where criminals use shielded transactions to anonymize illicit funds before moving them into fiat currencies via exchanges (Zhang et al., 2020).

9.2.3 Actionable Recommendations

- **Further Research into Privacy Coin Analysis**: More research is needed to develop innovative forensic techniques that can effectively penetrate the anonymity of privacy coins like Monero and Zcash. Collaboration between the private sector, academic institutions, and governments will be critical to make progress in this area (Koerhuis et al., 2020).
- **Continued Investment in Metadata Analysis**: Metadata analysis, such as scrutinizing off-chain behavior, should be a focus of future forensic research. This will help investigators trace privacy coins despite their inherent anonymity features (Zhang et al., 2024).

9.3 Real-Time Monitoring and Predictive Analytics

9.3.1 Lessons Learned

- **Real-Time Monitoring**: The development of real-time monitoring has become critical in blockchain forensics. It allows law enforcement and forensic firms to track cryptocurrency transactions as they occur, providing immediate insight into suspicious activities and enabling swift responses (McShane, 2023).
- **Predictive Analytics for Crime Prevention**: Predictive analytics models, powered by machine learning algorithms, have proven effective in forecasting potential criminal activities by analyzing historical transaction data. These models can flag emerging threats, such as new mixing services or unusual transaction flows, before they are widely adopted by criminals (Dunsin et al., 2024).

9.3.2 Key Strategies

- **Leveraging Predictive Models**: Forensic platforms should expand their use of predictive analytics to help authorities anticipate new criminal tactics. By monitoring dark web advertisements and correlating findings with transaction histories, investigators can identify potential threats early (McShane, 2023).
- **Combining Postmortem and Live Forensics**: Traditionally, blockchain forensics focused on postmortem analysis—reconstructing transactions after a crime had

occurred. However, live forensic tools now provide real-time alerts, allowing investigators to take preemptive actions, such as stopping the laundering of illicit funds (Varun, 2024).

9.3.3 Actionable Recommendations

- **Expand Real-Time Monitoring Capabilities**: Governments and private forensic firms should invest in expanding real-time monitoring across a wider range of blockchains. This will enable faster detection of illicit activities and help law enforcement agencies respond before transactions can be obscured (Shukla & Rathore, 2024).
- **Further Integrate Predictive Analytics**: The predictive capabilities of AI and ML should be continuously developed to allow investigators to forecast criminal behavior and take preemptive actions, enhancing the effectiveness of blockchain investigations (Dunsin et al., 2024).

9.4 The Future of Blockchain Forensics: Overcoming Cryptographic Barriers

9.4.1 Lessons Learned

- **Cryptographic Challenges**: Emerging cryptographic technologies, such as zero-knowledge proofs (ZKPs), homomorphic encryption, and quantum-resistant blockchains, are creating new challenges for blockchain forensics. These technologies enhance user privacy, making it increasingly difficult for investigators to trace transactions or identify suspects (Shashidhara et al., 2024).
- **Zero-Knowledge Proofs**: ZKPs, used in privacy coins like Zcash, allow transactions to be verified without revealing details about the sender, receiver, or amount involved. This creates a formidable challenge for forensic experts seeking to track the flow of illicit funds (Banerjee et al., 2020).

9.4.2 Key Strategies

- **Developing Solutions for ZKPs**: Forensic experts need to focus on developing techniques that can track the movement of funds between shielded and unshielded transactions, despite the strong privacy features of ZKPs (Banerjee et al., 2020).
- **Adapting to Quantum-Resistant Cryptography**: As quantum computing evolves, new quantum-resistant cryptographic techniques are being developed. Law enforcement agencies and forensic firms must adapt by focusing on these advancements, which will soon become integral to blockchain forensics (Ajala et al., 2024).

9.4.3 Actionable Recommendations

- **Invest in Research for Cryptographic Technologies**: Governments and the private sector must continue investing in research to overcome the challenges posed by cryptographic advancements like ZKPs and homomorphic encryption. Collaboration with academic institutions and cryptographic researchers will be essential (Atlam et al., 2024).
- **Prepare for Quantum Computing**: As quantum computing becomes a reality, blockchain forensic firms must prepare for the impact it will have on encryption techniques. Developing quantum-resistant blockchain tools will be critical for staying ahead of criminals who exploit quantum capabilities (Ajala et al., 2024).

10 International Cooperation in Combating Cross-Border Child Exploitation

The global reach of the Internet, particularly the Dark Web, has significantly contributed to the increase in cross-border child exploitation crimes. Anonymizing technologies, cryptocurrencies, and decentralized platforms allow offenders to evade detection, presenting substantial challenges for law enforcement agencies. These criminal operations often span multiple countries, requiring international cooperation to effectively combat transnational crimes (Drennan, 2024).

10.1 The Global Nature of Cybercrimes Involving Children on the Dark Web

10.1.1 Lessons Learned

- **Global Spread of Offenders and Victims**: Child exploitation crimes on the Dark Web are inherently global in nature. Websites hosting illegal content may be based in one country, while perpetrators and victims are scattered across different regions. This global nature of operations is further complicated using cryptocurrencies for payments, allowing transactions to occur almost instantaneously across borders with minimal oversight (Adel & Norouzifard, 2024).
- **Anonymity of Dark Web Platforms**: Platforms such as Tor and I2P provide anonymity for offenders, making it difficult for law enforcement to track and apprehend criminals. The combination of these platforms with privacy-focused cryptocurrencies creates a safe haven for child exploitation networks to operate undetected (Raman et al., 2023).
- **Jurisdictional Boundaries**: The international dimension of child exploitation complicates jurisdictional boundaries. Different countries have varying levels of

legal enforcement and protection for children, creating loopholes that offenders can exploit. The inconsistency in legal frameworks further exacerbates delays in investigations, making harmonized international cooperation essential (Lee, 2023).

10.1.2 Key Strategies

- **Fostering International Collaboration**: Effective international cooperation is necessary to trace and dismantle child exploitation networks. This includes the exchange of intelligence, evidence, and resources between countries, ensuring that perpetrators are tracked across borders and brought to justice (Raman et al., 2023).
- **Harmonization of Legal Frameworks**: Law enforcement agencies must work together to harmonize legal frameworks for child exploitation crimes. By aligning regulations and enforcement standards, countries can reduce loopholes that allow perpetrators to evade detection and prosecution (Lee, 2023).

10.1.3 Actionable Recommendations

- **Improve Cross-Border Information Sharing**: Governments should establish systems that facilitate the swift exchange of intelligence and evidence related to child exploitation crimes across borders. This will help law enforcement agencies act quickly and collaboratively (Raman et al., 2023).
- **Harmonize Child Exploitation Laws**: Countries should work to harmonize legal definitions of child exploitation, penalties, and procedures for cross-border investigations. A consistent legal approach will simplify the process of prosecuting offenders globally (Lee, 2023).

10.2 The Need for Unified International Regulatory Frameworks

10.2.1 Lessons Learned

- **Inconsistent Enforcement**: One of the major obstacles in combating cross-border child exploitation is the lack of a unified international regulatory framework. Countries have different laws and levels of enforcement, which enables offenders to seek refuge in jurisdictions with weaker legal systems or less rigorous enforcement (Council of Europe, 2001).
- **Delays in Investigation**: Differences in data privacy laws, standards of evidence, and bureaucratic barriers often delay investigations. In some cases, legal blind spots exist where certain forms of child exploitation are not criminalized, or

countries lack the resources to investigate these crimes thoroughly (United Nations Office on Drugs and Crime, n.d.).

10.2.2 Key Strategies

- **Developing a Standardized Regulatory Framework**: A unified international regulatory framework is necessary to streamline the process of investigating and prosecuting cross-border child exploitation crimes. This would involve aligning definitions of child exploitation, penalties, and evidence-gathering procedures across countries (CORDIS, 2024).
- **Expediting Cross-Border Investigations**: A unified framework would allow for the swift exchange of evidence and intelligence between countries. This is critical when immediate action is required to prevent harm, as well as for the efficient prosecution of offenders (CORDIS, 2024).

10.2.3 Actionable Recommendations

- **Create a Unified Legal Approach**: Governments should collaborate to establish standardized definitions and penalties for child exploitation crimes. A unified legal framework will enable more effective cooperation in cross-border investigations and prosecutions (CORDIS, 2024).
- **Facilitate Faster Evidence Exchange**: Law enforcement agencies should work together to develop mechanisms for sharing digital evidence swiftly and securely across borders. This will help minimize delays caused by varying data privacy laws and other legal complexities (United Nations Office on Drugs and Crime, n.d.).

10.3 Cross-Border Case Collaborations: Insights from Major Operations

10.3.1 Lessons Learned

- **Operation Bayonet (AlphaBay Takedown)**: This operation highlights the importance of cross-border collaboration in dismantling child exploitation networks. AlphaBay, a large Dark Web marketplace, was shut down through coordinated efforts between law enforcement agencies from the USA, Europe, and Asia. These agencies arrested key individuals and seized cryptocurrency wallets linked to child exploitation (Europol, 2017).
- **Welcome to Video Investigation**: This case demonstrated the global scale of child exploitation on the Dark Web and the effectiveness of international cooperation in combating it. The operation, which involved law enforcement agencies from multiple countries, led to the arrest of 337 individuals across 38 countries and

the rescue of 23 children. By tracing cryptocurrency payments used to purchase illegal content, the investigation dismantled one of the largest child exploitation platforms (Office of Public Affairs, US Department of Justice, 2019).

10.3.2 Key Strategies

- **Using Blockchain Forensics in International Operations**: Both Operation Bayonet and the Welcome to Video investigation underscore the importance of blockchain forensic tools in tracking cryptocurrency transactions across borders. These tools enable law enforcement to follow the financial trails of offenders, leading to their arrest and prosecution (Europol, 2017).
- **Global Intelligence Sharing**: The success of these operations highlights the need for countries to share intelligence and collaborate in real-time. Coordinated efforts between law enforcement agencies across continents are crucial for dismantling transnational child exploitation networks (Office of Public Affairs, US Department of Justice, 2019).

10.3.3 Actionable Recommendations

- **Expand the Use of Blockchain Forensics**: Law enforcement agencies worldwide should invest in blockchain forensic tools and techniques to improve their ability to track cryptocurrency transactions linked to child exploitation. These tools should be integral to future international operations (Europol, 2017).
- **Strengthen International Task Forces**: Countries should continue to form and empower international task forces dedicated to combating cross-border child exploitation. Such task forces can coordinate real-time intelligence sharing and jointly conduct operations across jurisdictions (Office of Public Affairs, US Department of Justice, 2019).

10.4 Enhancing Global Cooperation for More Effective Detection and Prevention

10.4.1 Lessons Learned

- **Real-Time Intelligence Sharing**: Despite some success, there remains significant room for improvement in the real-time sharing of intelligence and forensic data among countries. Rapid information exchange is critical for tracking perpetrators who move quickly across borders to evade detection (Corbett & Danoy, 2022).
- **Capacity Building in Less-Developed Nations**: Many less-developed nations lack the technical expertise and resources to investigate cybercrimes involving children. These countries require assistance in developing forensic capabilities and acquiring advanced forensic tools, which can be facilitated by partnerships

with international organizations such as Interpol and Europol (Sarkar & Shukla, 2023; UNODC, n.d.).

10.4.2 Key Strategies

- **Global Intelligence Platforms**: Establishing secure, global platforms for sharing intelligence and forensic data will improve the speed and effectiveness of cross-border investigations. This will enable law enforcement agencies to act swiftly on real-time information about child exploitation networks (Corbett & Danoy, 2022).
- **Capacity Building through Partnerships**: Developed nations and international organizations should focus on capacity building in less-developed nations by providing technical support, training, and access to advanced forensic tools. Partnerships between international agencies can help bridge the gap in resources and expertise (Sarkar & Shukla, 2023; UNODC, n.d.).

10.4.3 Actionable Recommendations

- **Establish Real-Time Data-Sharing Systems**: Governments should collaborate to develop secure platforms for the rapid exchange of intelligence related to child exploitation. This will enhance the ability of law enforcement agencies to track and apprehend offenders quickly (Corbett & Danoy, 2022).
- **Invest in Capacity Building for Developing Nations**: International organizations such as Interpol and Europol should focus on building forensic capabilities in less-developed countries. This can be achieved by providing training, technical support, and access to advanced forensic technologies (Sarkar & Shukla, 2023; UNODC, n.d.).

11 Discussion and Recommendations

The rapid evolution of blockchain technologies, particularly privacy coins and anonymizing tools, has posed significant challenges for regulators and law enforcement agencies worldwide. These technologies, while offering privacy and decentralized financial transactions, have become tools for criminal activities such as child exploitation, money laundering, and drug trafficking. To effectively combat these activities, both forensic methodologies and policy frameworks need to evolve. The following recommendations focus on advancing forensic techniques, strengthening public–private partnerships, creating global regulatory frameworks, and addressing the technological gap between law enforcement and modern cybercriminals.

One of the most pressing challenges in blockchain forensics is the rise of privacy coins like Monero and Zcash, which are specifically designed to obscure transaction details, making them attractive for illegal activities. These cryptocurrencies employ sophisticated cryptographic techniques that hide transaction participants and amounts, presenting a formidable obstacle for law enforcement agencies. Traditional forensic tools are often inadequate to trace transactions conducted via privacy coins, necessitating more advanced techniques.

To address these challenges, future research should focus on developing new forensic methods that go beyond on-chain data. Techniques, such as off-chain data analysis, including the scrutiny of transaction timings, network behavior, and even IP addresses, can offer crucial insights into otherwise anonymized transactions. Innovations like timing attacks and metadata analysis have already shown promise in narrowing down the origins of illicit transactions, even in highly secure privacy-focused environments. However, these advancements will require close collaboration among blockchain forensic experts, cryptographers, and academic researchers. Only through shared knowledge and innovation can breakthroughs in privacy coin forensics be achieved without compromising the underlying cryptographic protections of these blockchain systems.

While the development of cutting-edge forensic tools is essential, public–private partnerships play a critical role in facilitating the timely tracing of cryptocurrency transactions. Firms like Chainalysis, Elliptic, and CipherTrace have already been instrumental in providing law enforcement agencies with real-time analytics and tracing tools. However, the effectiveness of these partnerships is often hindered by delays in intelligence sharing. Investigations are frequently slowed down by bureaucratic hurdles or the reluctance of private firms to share proprietary data. Moreover, privacy laws further complicate the exchange of critical information.

To overcome these obstacles, it is essential to establish formal data-sharing agreements between private forensic firms and government agencies. These agreements must ensure that intelligence can be shared swiftly while adhering to privacy laws that protect individual rights. Additionally, many law enforcement agencies lack the technical expertise required to effectively investigate blockchain-based crimes. Joint training programs between public agencies and private firms can address this gap, ensuring that law enforcement officers are well-versed in the latest forensic tools and methodologies. With a skilled workforce, law enforcement can better leverage forensic tools and respond more effectively to emerging cyber threats.

Another significant challenge lies in the lack of a unified global regulatory framework for cryptocurrencies. Each nation has developed its approach to cryptocurrency regulation, with some enforcing strict controls and others allowing more lenient oversight. These disparities create opportunities for criminals to exploit regulatory gaps, shifting their activities to countries with weaker enforcement mechanisms.

To address this, a coordinated global response is essential. Future policy development should prioritize the creation of a comprehensive international framework for cryptocurrency regulation. Such a framework would need to clearly define cryptocurrencies under international law, establish consistent methods for identifying suspicious transactions, and set penalties for violating anti-money laundering (AML)

and counter-terrorism financing (CTF) regulations. Additionally, this global framework must ensure that cryptocurrency exchanges implement mandatory Know Your Customer (KYC) procedures and adhere to strict compliance standards across jurisdictions. International organizations, such as the Financial Action Task Force (FATF), should take the lead in promoting the adoption of these standards and ensuring their consistent application across borders.

As blockchain technologies continue to advance, law enforcement agencies face a growing divide between the tools used by criminals and their ability to combat illicit activities. Decentralized finance (DeFi) platforms, privacy-enhancing technologies, and new cryptographic innovations are pushing the boundaries of what is possible within the blockchain ecosystem. Law enforcement must adapt quickly, upgrading their tools and methods to keep pace with these developments.

One key area for future research is the integration of artificial intelligence (AI) and machine learning (ML) into forensic platforms. AI and ML can process vast amounts of data far more efficiently than manual analysis, identifying patterns and flagging high-risk transactions in real time. This will be particularly valuable in cases involving complex schemes such as ransomware attacks or large-scale fraud, where quick responses are critical. However, simply having the tools is not enough. Law enforcement must also have the expertise to use these tools effectively. Collaboration between law enforcement agencies, technology firms, universities, and forensic experts will be essential to bridge the gap between technology and law enforcement capabilities.

Additionally, policy development should focus on crafting legal frameworks that empower law enforcement agencies to seize cryptocurrency assets, freeze illicit funds, and compel exchanges to cooperate during investigations. These frameworks must strike a careful balance, ensuring that law enforcement has the necessary authority to act swiftly while safeguarding the rights of legitimate cryptocurrency users. Swift, yet ethical, responses will be crucial in future blockchain investigations, where the fast-paced nature of cryptocurrency transactions leaves little room for delays.

12 Conclusion

The fight against child exploitation on the dark web remains one of the most daunting challenges for modern law enforcement. By harnessing the power of blockchain forensics and fostering robust partnerships between public and private entities, significant strides have been made in tracking illicit activities and dismantling criminal networks. However, as technology continues to evolve—particularly with the rise of privacy coins, decentralized platforms, and anonymizing tools—law enforcement must remain vigilant, continually innovating to keep up with these emerging threats.

Case studies such as Operation Bayonet and the Welcome to Video takedown underscore the effectiveness of blockchain forensics in tracing cryptocurrency transactions and uncovering child exploitation rings. These examples also highlight the

indispensable role of international cooperation, where the ability to track money trails across borders is crucial in disrupting sophisticated, transnational criminal operations. Yet, the increasing adoption of privacy-focused cryptocurrencies like Monero presents new challenges, making investigations more complex and reinforcing the need for novel forensic tools and regulatory frameworks that can keep pace with these developments.

Blockchain forensics has proven to be a potent weapon in law enforcement's fight against cybercrime, offering previously inaccessible insights into illicit operations. By tracing the flow of cryptocurrency, investigators can map financial connections, identify perpetrators, and shut down illegal networks. However, the constant evolution of privacy-enhancing technologies demands that blockchain forensic capabilities continue to advance. To stay ahead of these challenges, continuous research and development of tools that can trace privacy coins, combined with the integration of artificial intelligence (AI) and machine learning (ML), will be essential in increasing the efficiency and speed of forensic investigations. AI and ML offer the potential to detect patterns more quickly and accurately, transforming the landscape of blockchain investigations by reducing the time it takes to follow transaction trails.

Looking to the future, several challenges and opportunities are on the horizon for blockchain forensics. The rise of decentralized finance (DeFi) platforms, in combination with privacy coins, introduces new obstacles for law enforcement, requiring innovative approaches to trace and analyze these transactions. Moreover, the establishment of a unified global regulatory framework for cryptocurrencies is critical. Such a framework would close legal loopholes that criminals currently exploit by operating in countries with weaker regulations. A globally coordinated effort will ensure that these technological advances do not outpace law enforcement's ability to combat cybercrime. The global nature of child exploitation requires coordinated international action. Strengthening public–private partnerships and encouraging collaboration between law enforcement agencies, blockchain forensic firms, and regulatory bodies is key to addressing the evolving technological threats posed by the dark web. Additionally, greater investment in research and development will ensure that forensic technologies remain at the cutting edge, equipped to respond to emerging challenges in cybercrime.

To sum up, eradicating child exploitation on the dark web demands a multifaceted global effort, one that prioritizes the advancement of blockchain forensics, the harmonization of international regulations, and the strengthening of cross-border collaboration. By continuing to work together, law enforcement agencies, forensic experts, and policymakers can dismantle these harmful networks and protect the most vulnerable members of society—our children.

References

Adel, A. and Norouzifard, M. (2024). Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application. *Big Data and Cognitive Computing* [online], 8(8), pp. 91–91. https://doi.org/10.3390/bdcc8080091.

Ajala, A., Arinze, A., None Onyeka Chrisanctus Ofodile, Okoye, C. and Ifesinachi, A. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, 10(1), pp. 321–329. https://doi.org/10.30574/msarr.2024.10.1.0038.

Atlam, H.F., Ekuri, N., Azad, M.A. and Lallie, H.S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics* [online], 13(17), pp. 3568–3568. https://doi.org/10.3390/electronics13173568.

Bahamazava, K. and Nanda, R. (2022). The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Science International: Digital Investigation*, 40, 301377. https://doi.org/10.1016/j.fsidi.2022.301377.

Banerjee, A., Clear, M. and Tewari, H. (2020). *Demystifying the Role of zk-SNARKs in Zcash* [online]. IEEE Xplore. https://doi.org/10.1109/AINS50155.2020.9315064.

Barbereau, T. and Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. *Computer Law & Security Review* [online], 49, 105829. https://doi.org/10.1016/j.clsr.2023.105829.

Celiksoy, E., Schwarz, K., Sawyer, L. and Ciucci, S. (2023). *Payment methods and investigation of financial transactions in online sexual exploitation of children cases Payment methods and investigation of financial transactions in online sexual exploitation of children cases 1 Payment methods and investigation of financial transactions in online sexual exploitation of children cases Content notice* [online]. Available from: https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/payment-methods-and-investigation-of-financial-transactions-in-online-sexual-exploitation-of-children-cases.pdf [Accessed 1 Oct. 2024].

Childs, A. (2025). How cryptomarket communities navigate marketplace structures, risk perceptions and ideologies amid evolving cryptocurrency practices. *Criminology & Criminal Justice, 25*(5), 1402–1419. https://doi.org/10.1177/17488958231213012

Corbett, S. and Danoy, J. (2022). *Beyond NOFORN: Solutions for increased intelligence sharing among allies* [online]. Atlantic Council. Available from: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/ [Accessed 1 Oct. 2024].

CORDIS, (2024). *European Informatics Data Exchange Framework for Courts and Evidence* [online]. CORDIS | European Commission. Available from: https://cordis.europa.eu/project/id/608185/reporting [Accessed 2 Oct. 2024].

Council of Europe, (2001). *European Treaty Series -No. 185* [online]. Available from: https://rm.coe.int/16800cce5b [Accessed 2 Oct. 2024].

Dasaklis, T.K. and Malamas, V. (2023). A Review of the Lightning Network's Evolution: Unraveling Its Present State and the Emergence of Disruptive Digital Business Models. *Journal of Theoretical and Applied Electronic Commerce Research* [online], 18(3), pp. 1338–1364. https://doi.org/10.3390/jtaer18030068.

De Lucci, A., De Lucci, F., Caringella, M., Galantucci, S. and Costantini, M. (2024). BACH: A Tool for Analyzing Blockchain Transactions Using Address Clustering Heuristics. *Preprint - Computer Science and Engineering*. https://doi.org/10.20944/preprints202406.1956.v1.

Department of Justice, (2017). *AlphaBay, the Largest Online 'Dark Market,' Shut Down* [online]. www.justice.gov. Available from: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [Accessed 2 Oct. 2024].

Diro, A., Zhou, L., Saini, A., Kaisar, S. and Hiep, C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities.

Journal of Information Security and Applications, 80, pp. 103678–103678. https://doi.org/10.1016/j.jisa.2023.103678.

Divakarmurthy, P., Requião da Cunha, B., Passold, J. F., Oliveira, M., & Menezes, R. (2024). Unravelling the dynamics of child sexual exploitation material circulation on the Dark Web. *PloS one, 19*(7), e0306516. https://doi.org/10.1371/journal.pone.0306516

Dondjio, I., & Themistocleous, M. (2021, December). Blockchain technology and waste management: A systematic literature review. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 194–212). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-85969-5_13

Dondjio, I., & Kazamias, A. (2023, December). A Blockchain framework for digital asset ownership and transfer in succession. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 88–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-17895-2_7

Drennan, I. (2024). *Dangerous shifts in the rapidly evolving world of online child sexual abuse - WeProtect Global Alliance* [online]. WeProtect Global Alliance. Available from: https://www.weprotect.org/blog/urgent-global-action-needed-to-stop-increasing-threats-to-children-online/ [Accessed 2 Oct. 2024].

Dunsin, D., Ghanem, M.C., Ouazzane, K. and Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation* [online], 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675.

EUROPOL, (2021). *Cryptocurrencies: Tracing the Evolution of Criminal Finances* [online]. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [Accessed 2 Oct. 2024].

Europol, (2017). *Massive blow to criminal Dark Web activities after globally coordinated operation* [online]. Europol. Available from: https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation [Accessed 2 Oct. 2024].

Europol, (2020, September 22). International sting against dark web vendors leads to 179 arrests. https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests

Europol, (2024). *Partners & Collaboration* [online]. Europol. Available from: https://www.europol.europa.eu/partners-collaboration [Accessed 2 Oct. 2024].

FBI, (2017). *AlphaBay Takedown* [online]. Federal Bureau of Investigation. Available from: https://www.fbi.gov/news/stories/alphabay-takedown [Accessed 2 Oct. 2024].

FBI, (2020). *Operation DisrupTor* [online]. Federal Bureau of Investigation. Available from: https://www.fbi.gov/news/stories/operation-disruptor-jcode-shuts-down-darknet-drug-vendor-092220 [Accessed 2 Oct. 2024].

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C. and Pesch, (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, 200902. https://doi.org/10.1016/j.fsidi.2019.200902.

George, S.J. (2023). Securing the Future of Finance: How AI, Blockchain, and Machine Learning Safeguard Emerging Neobank Technology Against Evolving Cyber Threats. pp. 54–66. https://doi.org/10.5281/zenodo.10001735.

Hamilton, R. and Leuprecht, C. (2024). The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions. *Ius gentium*, pp. 15–42. https://doi.org/10.1007/978-3-031-59543-1_2.

Him, I. (2024). *The Role of Cryptocurrency in Cybercrime: Tracking Transactions and Uncovering Networks* [online]. Available from: https://www.researchgate.net/publication/382176440_The_Role_of_Cryptocurrency_in_Cybercrime_Tracking_Transactions_and_Uncovering_Networks [Accessed 2 Oct. 2024].

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2022). *Cybercrime and Digital Forensics: An Introduction.* Abingdon, Oxon [UK]: Routledge.

Human Trafficking Front, (2023). *Cryptocurrency Use in the Online Sexual Exploitation of Children* [online]. Human Trafficking Front. Available from: https://humantraffickingfront.org/cryptocurrency-use-in-the-online-sexual-exploitation-of-children/ [Accessed 2 Oct. 2024].

International Centre for Missing & Exploited Children (ICMEC), (2021). *Cryptocurrency and the Trade of Online Child Sexual Abuse Material* [online]. Available from: https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf [Accessed 2 Oct. 2024].

Japinye, A.O. (2024). Integrating Machine Learning in Anti-Money Laundering through Crypto: A Comprehensive Performance Review. *European journal of accounting, auditing and finance research*, 12(4), pp. 54–80. https://doi.org/10.37745/ejaafr.2013/vol12n45480.

Kaur, S. and Randhawa, S. (2020). Dark Web: A Web of Crimes. *Wireless Personal Communications* [online], 112(1). https://doi.org/10.1007/s11277-020-07143-2.

Kim, M., Lee, J., Kwon, H. and Hur, J. (2022). Get off of Chain: Unveiling Dark Web Using Multilayer Bitcoin Address Clustering. *IEEE Access*, 10, pp. 70078–70091. https://doi.org/10.1109/access.2022.3187210.

Koerhuis, W., Kechadi, T. and Le-Khac, N.-A. (2020). Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Science International: Digital Investigation*, 33, 200891. https://doi.org/10.1016/j.fsidi.2019.200891.

Lee, M. (2023). *International Child Abuse and Exploitation: Understanding the Global Context* [online]. NCACIA Protection. Available from: https://www.ncacia.org/post/international-child-abuse-and-exploitation-understanding-the-global-context [Accessed 2 Oct. 2024].

Leonid, G. and Vladimir, G. (2023). Machine Learning in Classifying Bitcoin Addresses. *The Journal of Finance and Data Science* [online], 9, 100109. https://doi.org/10.1016/j.jfds.2023.100109.

McShane, J.J. (2023). *In-Depth Look at Chainalysis, Elliptic, and CipherTrace: Forensic Science in Blockchain Analysis* [online]. The Truth About Forensic Science. Available from: https://thetruthaboutforensicscience.com/in-depth-look-at-chainalysis-elliptic-and-ciphertrace-forensic-science-in-blockchain-analysis/ [Accessed 2 Oct. 2024].

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins: Characterizing payments among men with no names. *Communications of the ACM, 59*(4), 86–93. https://doi.org/10.1145/2896384

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A. and Christin, N. (2018). An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies* [online], 2018(3), pp. 143–163. https://doi.org/10.1515/popets-2018-0025.

Nazah, S., Huda, S., Abawajy, J. and Hassan, M.M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE Access*, 8, pp. 171796–171819. https://doi.org/10.1109/access.2020.3024198.

Ncube, T. and Kabwe, R. (2023). The regulation of cryptocurrencies to combat money laundering crimes in South African banking institutions. *De Jure* [online], 56(1), pp. 354–375. https://doi.org/10.17159/2225-7160/2023/v56a22.

Nicholls, J., Kuppa, A. and Le-Khac, N. (2024). The next phase of identifying illicit activity in Bitcoin. *International Journal of Network Management*. https://doi.org/10.1002/nem.2259.

Office of Public Affairs, US Department of Justice, (2019). *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, which Was Funded by Bitcoin* [online]. Justice.gov. Available from: https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child [Accessed 2 Oct. 2024].

Patsakis, C., Politou, E., Alepis, E. and Hernández-Castro, J. (2023). Cashing out crypto: state of practice in ransom payments. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00766-z.

Pinna, A., Tonelli, R., Orrú, M. and Marchesi, M. (2018). A Petri Nets Model for Blockchain Analysis. *The Computer Journal*, 61(9), pp. 1374–1388. https://doi.org/10.1093/comjnl/bxy001.

Qin, F., Wu, Y., Tao, F., Liu, L., Shi, L. and Miller, A.J. (2022). Multi-input address incremental clustering for the Bitcoin blockchain based on Petri net model analysis. *Digital Communications and Networks*. https://doi.org/10.1016/j.dcan.2022.09.003.

Raman, R., Kumar Nair, V., Nedungadi, P., Ray, I. and Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon* [online], 9(11), e22269. https://doi.org/10.1016/j.heliyon.2023.e22269.

Raman, S. and Shults, A.M. (2020). *Cryptocurrency Enforcement Framework* [online]. Available from: https://www.justice.gov/d9/pages/attachments/2021/01/20/cryptocurrency_white_paper.final_.pdf [Accessed 2 Oct. 2024].

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, 6, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313.

Salisu, S. and Filipov, V. (2023). Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation. *International Conference on Cyber Warfare and Security*, 18(1), pp. 338–347. https://doi.org/10.34190/iccws.18.1.947.

Sarkar, G. and Shukla, S.K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 2(1), 100034. https://doi.org/10.1016/j.jeconc.2023.100034.

Shahzad, M.F., Xu, S., Lim, W.M., Hasnain, M.F. and Nusrat, S. (2024). Cryptocurrency awareness, acceptance, and adoption: The role of trust as a cornerstone. *Humanities and Social Sciences Communications* [online], 11(1), pp. 1–14. https://doi.org/10.1057/s41599-023-02528-7.

Shashidhara, R., Chirakarotu Nair, R. and Kumar Panakalapati, (2024). Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions. *Security and Privacy*. https://doi.org/10.1002/spy2.461.

Shiva, M., Matsu, J., Ishibashi, Y. and Rosenbach, F. (2023). *Exploring Blockchain Technologies for Collaboration and Partnerships Title Acknowledgements* [online]. Available from: https://golab.bsg.ox.ac.uk/documents/exploring-blockchain-technologies-for-collaboration-and-partnerships.pdf [Accessed 2 Oct. 2024].

Shukla, D. and Rathore, M. (2024). *Real-Time Cryptocurrencies Monitoring for Criminal Activity Detection: A Comprehensive System* [online]. Available from: https://hdiac.org/articles/real-time-cryptocurrencies-monitoring-for-criminal-activity-detection-a-comprehensive-system/ [Accessed 2 Oct. 2024].

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J. and Salas, A. (2020). *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes* [online]. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4418/RAND_RR4418.pdf.

Spalevic, Z. and Ilic, M. (2017). The use of dark Web for the purpose of illegal activity spreading. *Ekonomika*, 63(1), pp. 73–82. https://doi.org/10.5937/ekonomika1701073s.

Tharani, J.S., Yougarajah, E., Hou, Z., Palaniswami, M. and Muthukkumarasamy, V. (2021). Graph Based Visualisation Techniques for Analysis of Blockchain Transactions. In: *IEEE 46th Conference on Local Computer Networks (LCN)*. https://doi.org/10.1109/lcn52139.2021.9524878.

Tuli, F.A. and Thaduri, U.R. (2023). The Integration of Artificial Intelligence in Forensic Accounting: A Game-Changer Asian Accounting and Auditing Advancement. *Asian Accounting and Auditing Advancement*, 14(1), pp. 12–20.

US Attorney's Office, Eastern District of North Carolina, (2024). *Investment Fraud Disrupted by Seizure of $5 Million in Cryptocurrency* [online]. Justice.gov. Available from: https://www.justice.gov/usao-ednc/pr/investment-fraud-disrupted-seizure-5-million-cryptocurrency [Accessed 1 Oct. 2024].

U.S. House Committee on Financial Services Democrats, (2024). Testimony of Michael Mosier Before the US House Financial Services Committee, Subcommittee on Digital Assets, Financial Technology and Inclusion. In *Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity*. Available from: https://democrats-financialservices.house.gov/uploadedfiles/hhrg-118-ba21-wstate-mosierm-20240215.pdf [Accessed 1 Oct. 2024].

United Nations - Office on Drugs and Crime, (n.d.). *True Crime Story - AlphaBay* [online]. United Nations: Office on Drugs and Crime. Available from: https://www.unodc.org/unodc/en/untoc20/truecrimestories/alphabay.html.

United Nations Office on Drugs and Crime, (n.d.). *Cybercrime Module 12 Key Issues: Online Child Sexual Exploitation and Abuse* [online]. Available from: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html.

UNODC, (n.d.). *Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms* [online]. www.unodc.org. Available from: https://www.unodc.org/e4j/zh/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html.

UNODC, (2022). *Digest of Cyber Organized Crime Second Edition* [online]. Available from: https://www.unodc.org/documents/organized-crime/tools_and_publications/Digest_of_Cyber_Organized_Crime_2nd_edition_English.pdf.

UNODC and WACAP, (2020). *WACAP: Cornerstone of International Cooperation 'Cooperating across borders to effectively tackle transnational organized crime' West African Network of Central Authorities and Prosecutors against Organized Crime* [online]. Available from: https://www.unodc.org/res/organized-crime/gptoc_news-and-events_ninth-wacap-plenary-meeting_html/BROCHURE_COMPILATION_OF_SUCCESS_STORIES_-_English.pdf.

US Department of Justice, (2020). *International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million* [online]. www.justice.gov. Available from: https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170.

Uzougbo, S., Ikegwu, G. and Adewusi, N.A.O. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. *Magna Scientia Advanced Research and Reviews*, 11(1), pp. 068–083. https://doi.org/10.30574/msarr.2024.11.1.0075.

Varun, V. (2024). Prospects and Models of Combating Cryptocurrency Crimes: The India-EU Dialogue as a Perspective? *Eucrim*. https://doi.org/10.30709/eucrim-2023-032.

Wei, Z., Fang, J., Hong, Z., Zhou, Y., Ma, S., Zhang, J., Liang, C., Zhao, G. and Tang, H. (2024). Privacy Protection Method for Blockchain Transactions Based on the Stealth Address and the Note Mechanism. *Applied Sciences* [online], 14(4), 1642. https://doi.org/10.3390/app14041642.

Wijaya, D.A., Liu, J.K., Steinfeld, R., Liu, D. and Yu, J. (2019). On the Unforkability of Monero. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. https://doi.org/10.1145/3321705.3329823.

Wu, Y., Tao, F., Liu, L., Gu, J., Panneerselvam, J., Zhu, R. and Shahzad, M.N. (2021). A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation. *IEEE Transactions on Network Science and Engineering*, 8(2), pp. 1230–1241. https://doi.org/10.1109/tnse.2020.2970113.

Zhang, J., Cai, K. and Wen, J. (2024). A Survey of Deep Learning Applications in Cryptocurrency. *iScience*, 27(1), pp. 108509–108509. https://doi.org/10.1016/j.isci.2023.108509.

Zhang, Z., Li, W., Liu, H. and Liu, J. (2020). A Refined Analysis of Zcash Anonymity. *IEEE Access*, 8, pp. 31845–31853. https://doi.org/10.1109/access.2020.2973291.

Interpol's Crucial Role in Tackling Child Exploitation on the Dark Web



Amer Fakhoury

1 Introduction

International organizations, specifically the United Nations and its affiliated branches, play an important role in combating crime. Crimes have significantly increased in our contemporary society, and the internet has become an important tool for criminals to commit their offenses, which now affect all aspects of our lives. The internet is no longer just a means of spreading legal, cultural, economic, and social knowledge; it has also become a tool for spreading criminal ideas and committing crimes beyond what anyone could imagine. One of the most significant crimes that has become widespread in our time is the exploitation of children through the internet.

Child exploitation, especially over the internet, has become one of the most serious global challenges of the modern digital world. The most sinister aspects of this crime are how it is carried out on dark web platforms, which are a part of the internet used to hide criminal activities such as the distribution of child sexual abuse material (CSAM) (Europol, 2020). These platforms provide anonymity to offenders, making it very difficult for national law enforcement agencies to track down criminals. This crime has become one of the most the lucrative forms of cybercrime (Save the Children, 2013). The internet has become divided into two completely different worlds: the visible world, accessible to everyone, where people can benefit from the internet in various ways, and the hidden, dark world where all types of criminal activities and evils, beyond human imagination, are widespread.

To address these challenges effectively, the United Nations Office on Drugs and Crime (UNODC) states that there are certain types of crimes that cannot be combated without international cooperation, as criminals are often in one country while the victims are in another (UNODC, 2021). Consequently, the need for international

A. Fakhoury (✉)
American University in the Emirates, Dubai, United Arab Emirates
e-mail: amer.fakhoury@aue.ae

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_4

cooperation becomes evident between countries and law enforcement agencies is no longer just a simple need, but rather an urgent necessity for all member states of the United Nations to combat crime. Interpol's structure, consisting of 195 member states, has been very helpful in coordinating efforts to combat child exploitation on an international scale (Interpol, 2023). No region on the surface of the Earth is isolated from this type of crime. There is no geographical spot on any of the known continents where such crimes have not occurred. Thus, Interpol's involvement becomes critical as no country in the world can claim to be able to combat these crimes without real cooperation among the member states of Interpol. Given these complexities, there is an urgent need for these countries to collaborate, share ideas, and exchange information in order to put an end to these crimes, which are considered some of the most heinous that humanity has ever known. For that reason, this paper examines how Interpol uses resources, technologies, and partnerships with national and international agencies to put an end to child exploitation networks on the dark web.

Research Problem Statement

Child sex exploitation on the dark web is unfortunately a global crime, fed and hidden from view by anonymity and technical hurdles that defeat domestic law enforcement agencies. The pursuit of justice does continue across borders by Interpol but due to the technological lag, legal discrepancies in countries, and unsuccessful cooperation at international levels, these crimes remain uncontrolled. This study examines the indispensable role Interpol plays in coordinating resources, partnerships, and technology to take down hidden child exploitation networks located on the dark web.

2 Overview of Interpol

Interpol Mission and Structure:

In 1923, Interpol was set up to help in global criminal investigations (Interpol, 2022). Its goal is to allow police forces around the world share information and work across borders, fighting transnational threats such as cybercrime, human trafficking, and terrorism. This is an organization that provides a hub for exchanging information within the police, allowing law enforcement to work together in harmony and effectively (Harkin, 2021).

Focus on Cybercrime and Child Exploitation:

One of the most famous international organizations, which is part of United Nations Organisation (UNO), is Interpol, which plays a critical role in investigating cybercrimes and online crimes such as child exploitation. The Crimes Against Children Unit is responsible for investigating crimes involving the online sexual exploitation of children using current digital technology and international resources. The

unit plays a crucial role in locating offenders, disrupting exploitation networks, and saving victims around the world (Interpol, 2021).

3 The Dark Web and Child Exploitation

What is the Dark Web?

The dark web refers to the part of the internet that is not indexed by traditional search engines and can only be accessed using specific software (Babak Akhgar and others, 2021). According to Brett Lee, a former undercover internet detective and police office (Brett Lee, 2018): the internet's way bigger than most people realize. When we think about life online, we usually just consider the huge, well-known sites and apps from big companies and organizations—Facebook, YouTube Google, and Wikipedia. In light of these challenges, it's hard to wrap your head around the idea that the public internet—with its billions of pages a quick Google search away—is merely the tip of the iceberg. These easily accessible websites are what some call the Surface Web and even with the sheer number of public surface websites, they still only account for a tiny slice of the internet's total content and data. In fact, experts estimate the Surface Web is just 4% of the whole internet. The other 96% is tucked away as dark data and Deep Web pages." Dark Web is often used for illegal activities, including child exploitation, drug trafficking, and weapon sales. Due to its anonymity, it becomes challenging for law enforcement agencies to track down criminals operating on the dark web (Europol, 2021).

Child Exploitation Trends on the Dark Web:

Indeed, use of the dark web is enabling child sexual exploitation to flourish. Several websites on the dark web sell Child sexual abuse material and operate these sites via a subscription-based model (ECPAT, 2022). To provide a basis for this study, it is important to look at findings already been established by NCMEC. According to recent report published in 2023 by the US National Centre for Missing and Exploited Children (NCMEC, 2024), over 36.2 million reports of suspected child sexual exploitation, which represents a 72% increase over the number of reports received in 2020.

The use of this material was enabled by the explosion in encrypted communication, which has made it increasingly difficult for law enforcement to track down its distributors (UNICEF, 2022).

The Dark Web Infrastructure and Anonymity Tools

To better understand the problematic of this research, it is important to say that the dark web is a part of the internet that cannot be accessed through standard browsers, only via special software, such as Tor, I2P (Invisible Internet Project), Freenet, ZeroNet or Tails OS (The Amnesic Incognito Live System), which encrypts and routes people traffic over multiple servers to hide their identities and locations. The dark

web is built to protect people from being followed, which also means it is a less secure environment for criminals who exploit children. That layered encryption makes it difficult for law enforcement to identify users or access content. Tools like Tor or I2P ensure anonymity of identities and locations, allowing perpetrators to spread illegal content, organize without detection, and outsmart the authorities—making it an extremely difficult task to disrupt these activities.

Challenges of Policing the Dark Web

Following a comprehensive review of the literature, the main trend discovered is that these challenges arise especially due to the anonymous profile of the dark web and the ethics involved in detecting criminal activity (Warner, 2023).

The dark web gives users the ability to access information, documents, and other content that would be difficult or impossible for national law enforcement agencies to track back or to *unmask the identities of perpetrators* (Finklea, 2018), owing largely in part their use of encryption technologies along with a cloak of anonymity which makes it extremely hard if not close on mission impossible for policing authorities worldwide. In addition, according to (UNODC, 2021), crime travels transnationally, and a country is not in the jurisdictional boundaries of another state directly exercised but have an international cooperation system like Interpol.

4 Interpol's Role in Tackling Child Exploitation

One of the many operations that Interpol headed successfully breaking down child exploitation networks located on the dark web. Interpol, for instance, noted that it has initiated several successful operations such as Operation Blackwrist that resulted in the arrest and identification of key individuals heading an international child exploitation ring (Interpol, 2019). According to information provided by Interpol website, over the last couple years, an international operation called Blackwrist led to 50 kids being saved from abuse. It also meant some sickos who were preying on little children got busted and charged in Thailand, Australia, and the USA. This whole thing started back in 2017 when Interpol found stuff showing 11 boys under 13 being molested. (Interpol, 2019). This operation, managed and coordinated by INTERPOL in collaboration with law enforcement agencies from several countries, serves as proof of the importance of international cooperation in putting an end to child exploitation crimes. Without this cooperation, the organization would not have been able to dismantle one of the largest child exploitation networks on the internet in modern history, or as (Chertoff, 2021) says that: "There is no doubt this operation highlighted the need for global efforts when working out who should be accountable to pursue criminals through borders and save victims in different parts of the world". Here, I want to emphasize the fact that these criminals who were apprehended must serve as a lesson to other offenders who use the internet. Through this research, I express my full satisfaction with the punishment imposed on those I refer to as the "killers of childhood". According to many news (straits times, 2019), Salangam was

sentenced to 146 years in prison by Thai courts, while an associate, a pre-school teacher, got 36 years. Tokputza was handed a 40-year prison term at his trial in Australia, the longest for child sex offences in the country.

Darknet Digital Forensics and Advanced Tracking Technologies from Interpol

Using a broad range of advanced technologies and forensic science, information is collected by Interpol on the dark web that assists them in fighting against child exploitation. For example: Blockchain analysis software traces illicit cryptocurrency transactions. Furthermore, Interpol uses natural language processing (NLP) and sentiment analysis to track conversations related to exploitation in dark web forums. Graph analysis tools such as that of Palantir posts map of criminal networks, and digital profiling links suspect across platforms. Coupled with open-source intelligence (OSINT) and AI-based behaviour analysis, these technologies help Interpol monitor, identify, and destroy networks of child exploitation in the hidden online world.

International Child Sexual Exploitation (ICSE) Database:

The ICSE (International Child Sexual Exploitation image and video database) was developed by Interpol as an intelligence and investigative tool, enabling specialized investigators to share data on child sexual abuse. According to (Interpol, 2024), Investigators can instantly link the victims, abusers, and locations by comparing images and videos with software. It helps in preventing resources from being wasted by notifying investigators early if similar series of images have already been found or identified in another county, and assists they no longer need to spend precious time on comparing the number of possible matches. It also puts specialized investigators in over 70 countries within easy reach of their global counterparts from around the world via an information and data exchange initiative. Experts in victim identification can also use digital and visual/audio analysis of photographs and videos to pull out leads, look for commonalities across cases, and pool their investigative efforts to find the children who are being sexually exploited. INTERPOL's Child Sexual Exploitation database holds 4.9 million images and videos and has helped identify 42,300 victims worldwide.

Artificial Intelligence (AI) and Digital Forensics:

As a result of the technological advancements that have affected the international community and the implementation of artificial intelligence, Dark Web criminals have increasingly turned to AI to conceal their criminal activities and hide their identities. While these issues persist, it has become necessary for international organizations, specifically INTERPOL, to take this new challenge into consideration. Recently, Interpol used artificial intelligence (AI) and digital forensics to combat child exploitation on the dark web. AI algorithms help to analyse and decrypt files, enabling law enforcement to trace suspects and identify victims (Choo, 2019). Digital forensics techniques are also used to retrieve hidden information and map the networks of criminals operating anonymously on the dark web (Interpol, 2020). According to (Neha & Shailesh, 2022), digital security based on AI is of immense

benefit for the security industry. Thus, in response to the increasing use of AI and Machine Learning ML technologies, actions were taken against Dark Web (DW) crimes, and applications for crime recognition were developed.

Collaborations with National Law Enforcement Agencies:

Police cooperation with the help of Interpol is one of the main activities dealing with globalization and intricate transnational crimes, including human trafficking, drug trafficking, cybercrime, and for sure combatting child exploitation. As cooperation between countries covers a wide range of activities among the member states of Interpol. Combating transnational crimes, particularly the crime of child exploitation, cannot be achieved without the cooperation of law enforcement agencies among member states. This cooperation makes it easier for the flow of information so that the criminals can be apprehended, or any other unlawful activity be prevented. The coordination provided by Interpol and a real-time sharing of information among the different police forces in this regard is almost vital and indispensable for combating child exploitation. This also involves sharing of information about criminals, suspects, and offences, as well as forensic material that may be useful in international investigations. Interpol has many practical tools for combating international crimes, with one of the most important being the notices system. Interpol Notices are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information. These notices are issued by the General Secretariat at the request of a member country's Interpol National Central Bureau and are made available for all our member countries to consult in our Notices database. Operation like Jackal III, Blackwrist, Liberterra, INFRA, Angel Watch, Rescue, and Narsil, all are very successful ones targeting the most heinous crime. On the other hand, regional organizations that combat crimes against children, such as Europol, play an important role in fighting crime alongside Interpol. We mention here what happened in 2011 when Europol (Jardine, 2017) managed to dismantle one of the largest child exploitation networks on the internet, working together with 13 countries, Operation Rescue went down. This police crackdown turned up 670 suspects and busted 184 people for having kid abuse images and stuff (Europol, 2011). Then in July 2014 the National Crime Agency in the UK arrested, like, 650 persons for different crimes against enfants from just having photos to actually hurting them and northern Ireland got in on it too, finding 50 more creeps in 2015 and laying 37 charges. These are some times the cops took down paedophile rings hiding deep in the dark Web. The above coordination reflects the importance of cooperation between international and regional agencies in confronting these crimes.

5 Legal Considerations

Reflecting on the insights discussed, it becomes evident that, the dark web with the issue of jurisdiction being one of the principal challenges in policing the dark web. Dark web offenders are frequently based in other countries, and international

assistance is necessary when prosecuting such criminals. Given the global scale and complexity of this issue, international structures, such as the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography adopted in 2000. Furthermore, the Budapest Convention on Cybercrime covers a substantial resource for this sort of participation (Council of Europe, 2021), and the Lanzarote Convention adopted in 2007 by the Council of Europe relating to the Protection of Children against Sexual Exploitation and Sexual Abuse, requires criminalization of all kinds of sexual offences against children.

These jurisdictional limitations present unique challenges for law enforcement agencies such as Interpol. The divergence of privacy laws, restrictions on cross-border data flows, and standards of evidence between countries makes it harder to share what we need to know. Some countries have laws that protect even child sex offenders from having their online activity monitored when much worse crimes are in play. Moreover, the intricate nature of extradition can slow or halt any prosecution against those who commit crimes on dark web marketplaces, especially when countries do not have an extradition treaty in place, or if they have fundamentally different views regarding internet freedom and privacy. This leads to long delays in investigations and gives infringers time to utilize 'safe havens' within the law. Thus, the combination of a dark web, international cybercrime laws with no clear unifying standards on child sexual exploitation prosecutions across national borders, and courts restricted from cross-border data sharing has created an enforcement theme calling for harmonization of laws between countries to address these issues in concert.

6 Future Directions, Recommendations, and Conclusion

In summary, the findings highlight the importance to reinforce international cooperation to fight against child exploitation on the dark web. Interpol need be strengthened as a global police cooperation enabler in the realm of law enforcement information sharing and technical support new technologies, like AI and blockchain, could help strengthen the ability of law enforcement to identify and trace criminal activities on the dark web. You can find more details in our research, and we look forward to continued partnership with private tech companies when it comes to new tools against child exploitation. (UNODC, 2021).

Without Interpol and its endeavours, combating child abuse on the dark web would be impossible. It has brought down some of the largest child exploitation networks globally and saved thousands of lives through its operations, databases, and technological breakthroughs. Nevertheless, the features of obscurity and encryption technologies that enable these crimes are continually changing, which necessitates ongoing international efforts to cope with them.

To continue to make advances in the fight against child exploitation, it is necessary to observe the following recommendations:

1. What Interpol is not yet doing, but should, is to call for the development of a more coherent global legal regime on cybercrime and child Exploitation.
2. Strengthen the relationships with tech companies.
3. One possibility would be for Interpol to work with UN member states to forge cross-border data-sharing agreements that prioritize civil liberties while also enabling the exchange of evidence.
4. Create and maintain a special Interpol task force to focus on dark web child exploitation.

References

Babak Akhgar, Marco Gercke, Stefanos Vrochidis, Helen Gibson (2021). Dark Web Investigation. https://doi.org/10.1007/978-3-030-55343-2

Brett Lee, (2018). "Dark We Handbook". 180503_ebook_print_withLink.pdf(internetsafeeducation.com)

Chertoff, M. (2021). "Global Cybercrime and the Role of Interpol." *Policing and Society*.

Choo, K.-K. R. (2019). "Blockchain and AI Solutions in Cybercrime Policing." *Cybersecurity Journal*.

Council of Europe. (2021). "The Budapest Convention on Cybercrime." Council of Europe.

ECPAT. (2022). "Trends in Child Sexual Exploitation and Online Grooming." ECPAT International.

Europol. (2020). *Internet Organized Crime Threat Assessment 2020*. Europol.

Europol. (2021). *Dark Web and Online Child Exploitation*. Europol.

Finklea, K. M. (2018). "The Dark Web: Trends and Law Enforcement Solutions." U.S. Congressional Research Service.

Harkin, D. (2021). "The Global Policing of Cybercrime." *Journal of International Policing*.

https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201

https://www.interpol.int/en/How-we-work/Notices/About-Notices

https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

https://www.straitstimes.com/world/europe/50-children-saved-after-police-bust-paedophile-website-interpol

International Child Sexual Exploitation database (interpol.int)

Interpol. (2019). *Operation Blackwrist: Dismantling Child Exploitation Networks*. Interpol.

Interpol. (2020). *Crimes Against Children: Global Policing Efforts*. Interpol.

Interpol. (2021). *Crimes Against Children: Global Policing Efforts*. Interpol.

Interpol. (2022). *International Child Sexual Exploitation Database*. Interpol.

Interpol. (2023). "Crimes Against Children." Interpol. https://www.interpol.int;

Interpol. (2024). What is Interpol? https://www.interpol.int/en/Who-we-are/What-is-INTERPOL

Jardine E (2017) The dark web dilemma: Tor, anonymity and online policing. In: Cyber security in a volatile world. Centre for International Governance Innovation, pp. 37–50. http://www.jstor.org/stable/resrep05239.8

NCMEC (2024). Cyber Tipline 2023 Report. https://www.missingkids.org/cybertiplinedata

Neha, Shailesh, (2022) Artificial Intelligence and Machine Learning Algorithms in Dark Web Crime Recognition, In book: Using Computational Intelligence for the Dark Web and Illicit Behavior Detection (pp. 126-149)

Save the Children (2013). sInternet Child Exploitation, regional Report, April 2013. Internet-child-exploitation-april-2013.pdf(savethechildren.net)

UNICEF. (2022). *Child Exploitation in the Digital Age*. UNICEF.

United Nations Office on Drugs and Crime (UNODC). (2021). *The Global Study on Cybercrime.* UNODC.

Warner, C. (2023). Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical and Legal Issues. In: Montasari, R. (eds) Applications for Artificial Intelligence and Digital Forensics in National Security. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-40118-3_7

Using Artificial Intelligence Algorithms to Monitor Child Sexual Exploitation in the Dark Web Environment



Amar Yasser El-Bably

1 Dark Web Components

The dark web really reflects its name, as it can only be accessed by dedicated programs and specific means, and allows users to access the dark web anonymously while maintaining their complete privacy, the deep web is a huge virtual space that includes a huge amount of information that cannot be obtained when browsing the surface network, and provides the user with a high degree of privacy, but the challenge it poses is that it represents a successful way for those who invest in the exchange of illegal goods and materials. This requires the security services in all States to continue to monitor this network and devise renewed methods to monitor and deal with negative content as soon as possible, while ensuring the preservation of users' privacy, and of course, this requires high-level coordination between the various security agencies.[1]

2 The Genesis of the Dark Web

In the beginning, let's go back to the emergence of Internet technology in the twentieth century in 1960, where the idea was from a military entity, which is the US Department of Defense, and it was working on a research group under the

[1] Arpanet :she Computer Network One of the first networks Data transfer Using the technique of Packet Switching in the world, connected a number of universities and research institutions in United States, and used for scientific and academic purposes. It is the first nucleus For the Internet and the first data transmission network to be used Internet Protocol Package.

A. Y. El-Bably (✉)
Egyptian Police Academy, Cairo, Egypt
e-mail: 3marelbably@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_5

name[2] (Arpanet), which is a technology whose idea is to link physical devices to each other through protocols, with the aim of providing technology that facilitates them to transfer data and send and receive data, and this idea has succeeded, and the US Department of Defense By sending the first message from one device to another device in an antenna via e-mail in the seventies, and then appeared from here the innovation of the Internet, which facilitated a lot of work, efforts, work, and saving time, but it was not easy to deal with the Internet, so the person had to have high experience in the computer in order to be able only to send his message, and with the spread of the idea, many experts participated in the development of this project and until the thought of a person called (Tim Berners-Lee)[3] to expand the scope of the Internet and facilitate it for people to be a technology available to everyone and to help them in their work has invented what is known as the information network or the World Wide Web or what is abbreviated by www, and after Tim Berners published his idea, which changed the world because of the huge demand of users around the world for this new technology, which helps them very significantly in sending any data from any device to another device With ease, as Internet explorers appeared, which helped people more in dealing with the Web, which is one of the Internet services, and when this new technology spread in the world, a computer scientist named (David Shaum) said that the Internet has become a treasure trove of information about people, in short, it is possible through priority data or known as Meta Date to spy on anyone who uses the Internet or the Web, it is very easy to know the sender and sender The mechanism and the content of the message and here there must be some privacy, and the US Department of Defense has worked on a new project to provide privacy for Internet users and hide their identities, especially after the protection of information has become a basic thing and national security for governments around the world due to the content of that information of confidential documents that may be exploited by some other governments or organizations in work that causes crises in the future, so it was necessary for the US government to innovate something to protect this huge amount of data available everywhere on the Internet, and the computer scientist David said that “no one can be hidden on the Internet by himself, but this can be achieved if the number of users of this hidden network increases”, meaning that the more users there are, the more each person will be hidden on the Internet.

In 1999, Ian Clark,[4] a computer scientist at the University of Edinburgh in the United Kingdom, drew attention to flaws in the design of the Internet, which

[2] Amar y.elbably. Forecasting Cyber Crimes in the Age of the Metaverse : Societal Risks of Using Cyber Metaverse Technology at : https://www.igi-global.com/gateway/chapter/334497.

[3] Tim Berners-Lee Ho engineer And a computer scientist For the World English, invented, which is known as the web. He is now a professor of computer science, Wide Web at University of Oxford in United Kingdom, submitted a proposal for an informationmanagement system in March 1989, and succeeded in mid-November of the same year in the implementation of the first successful communication between a client and a servant For the hypertext transfer protocol accordance Service Request Form.

[4] https://www.merriam-webster.com/dictionary/dark%20web 30/7/2022 تاريخ الاطلاع.

was then only 10 years old, as Clark explained that using the general addressing system and routing programs that could be tracked, it was very easy to monitor and censor the "web", Clark believes that powerful entities such as governments or companies can use this information to control us, so Clark developed the "Freenet" network[5] To be a decentralized and anonymous alternative to the Internet, other networks soon followed with Tor and I2P (the hidden Internet project).

Together, these three networks constitute the dark web,[6] and there is no doubt that these networks affect due to the illegal websites and operations they contain such as (buying credit cards, selling narcotics, organ trafficking, arms trade, hacker programs, counterfeit currency, … etc.) in the national security and stability of countries, which called for many national institutions interested in security to study them and develop strategic plans to deal with them, and the idea of terrorist ideology to use the digital space, because the informational content of these sites is one of the most circulated information among the public, especially young people, as these sites were able to attract huge numbers of browsers in a short period of time, exceeding the capabilities of the media. The other traditional by a large margin, which gave it a great ability to influence the dissemination of extremist ideas and beliefs, especially among young people, and therefore the Internet has become containing three layers as follows:

First layer: Surface Web:
It is also known as the clean web, which is that part of the World Wide Web available to the general public and indexable and tabular through traditional search engines, where these search engines use programs called "crawlers", or "spiders", which link the surface web pages to the search engine and archive them[7] Everything is centralized and this means that when someone uses a website on the international information network, for example, a site of social networking sites Facebook, he leaves in the "servers" of Facebook images and text that remain in the Facebook information store, and if someone else wants to see this information, he must also register with Facebook,[8] and in this case, the Internet "servers" of

[5] Concept Freenet:he Open source software used to share peer-to-peer datavia Internet. While providing strict methods to protect privacy Freenet It exists on a decentralized network and is designed to allow freedom of expression without censorship. By enabling users to share data anonymously by sharing bandwidth and space Hard Drive (known as a data store), can be defined Freenet as the Internet within the Internet because users.

They are not .limited to Share files, but they can use Freenet For any purpose, the concept of Freenet To store programs and data originally by Ian Clarke, but Frenette has been evolving since 2000.

[6] https://www.alrab7on.com/everything-about-dark-web/ تاريخ الاطلاع 30/7/2022.

[7] World Data Website Internet Usage Report:
https://datareportal.com/reports/digital-2021-July-global-statshot.

[8] Essam Tawfiq Ahmed, Electronic Information Sources, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2015, p. 98.

Facebook is the store of texts and images of that person, and this from the point of view of data protection is what must whoever has access to Facebook, Google, and other large information companies can reveal the information of people in the memory of those servers.

Second layer: Deep Web:
By simple definition, they are everything that traditional search engines do not find, in other words, everything that is not found on the surface network, and represents about 96% of Internet content,[9] such as libraries, archives, corporate internal networks, private institutions, bank accounts, social networking sites and other major sites such as Google, Amazon, and others.

Third layer: dark web:
This layer is located within the deep network, and can be defined as the part of the deep network that was deliberately hidden and cannot be accessed through traditional search engines, due to what it contains information about hacking programs, spyware and others, it is a world that is not subject to any censorship, and controlling it is almost difficult, but not impossible, and within it there is information that is prohibited from circulation, which is punishable by law, such as the black market and sites teaching the manufacture and use of weapons and explosives, in the hidden Internet. There are no search engines such as Google, but the available pages are located according to a certain "catalogue" in which the old pages are not indexed, and the designers of the hidden Internet wanted to keep the data of the users of this network secret, which represents a world of the Internet that even the United States intelligence cannot access, access, or spy on.[10]

- The first layer is considered as the surface, and traditional search engines can access it, and the second layer does not include suspicious things, but it uses the "address" IP, without specifying a scope for it, which is difficult to access, and the third layer is the deepest, and is known by several names, including Deep Web, Deep Network, Hidden Internet, and Dark Web Dark Internet[11] as shown in the Fig. 1.

[9] Sameh Sabbour, Patterns of Use of Network Terrorism, Abu Dhabi, Future Center for Advanced Research and Studies, 2019, pp. 4, 5.

[10] Abdul Ghaffar Afifi, The Cyber Deterrence Strategy of the United States of America, Riyadh, College of Strategic and Security Sciences, Naif Arab University for Security Sciences, 2018, pp. 196–200.

[11] William Marcellino et al., Social Media Monitoring and Analysis: Through U.S. Department of Defense's Future Social Media Analysis in Support of Information Operations, RAND National Defense Research Institute, 2017, p. 33.

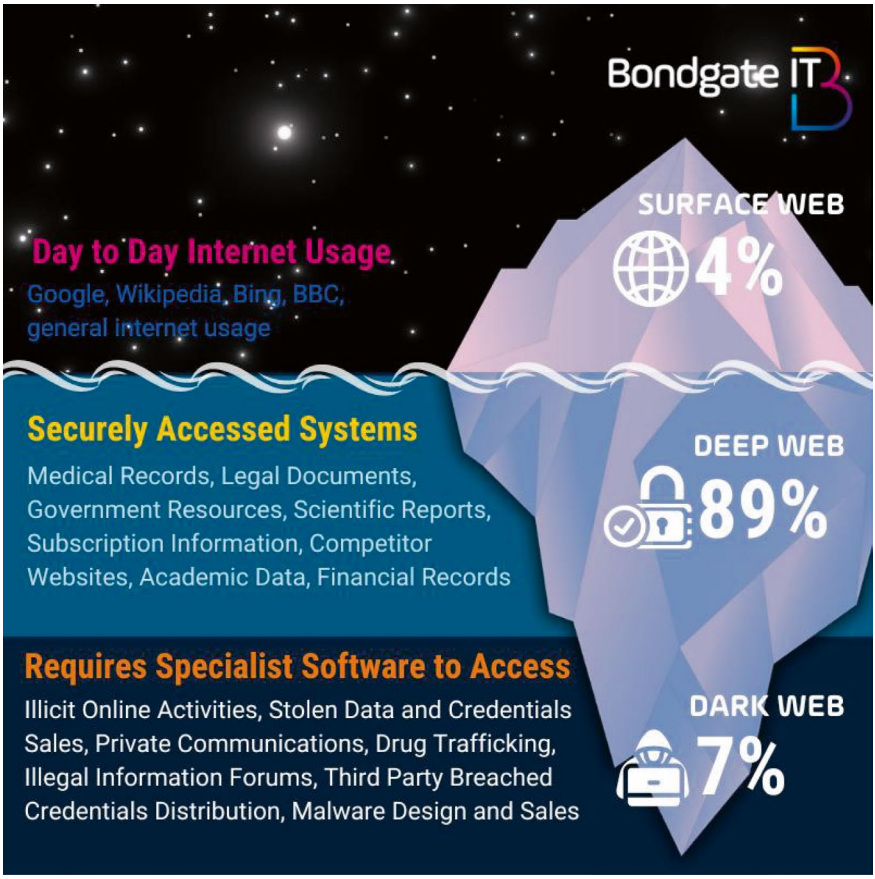


Fig. 1 Internet layers[12]

3 Second Branch

Uses of the dark web

The "deep web", the "dark web", the "dark web" is a virtual field that has become a concern for the security services in the world because it constitutes a space for trafficking in contraband, and an escape for many users who avoid censorship of their practices, which are usually outside the law. Its serious repercussions remain numerous on the security of States, but reducing them depends on the effectiveness of mechanisms and means[13] of confrontation.

[12] https://www.bondgate.co.uk/cybersecurity/dark-web-dangers-protecting-north-east-businesses/.

[13] Tarek Benhada, Hespress, Ahmed Youssef El-Tahawy, Electronic Evidence and its Role in Criminal Evidence, Cairo, Dar Al-Nahda Al-Arabiya, 2015, pp. 21–23.

The dark web is a way to achieve a level of anonymity on the Internet; it is a term that refers to websites that block IP addresses from the servers through which they are published, making it impossible to know the identity of the sites, or those in charge of them, as it does not appear on search engines, such as Google, and can be defined as: that part of the deep web that was deliberately hidden, and cannot be accessed through traditional search engines, and it is the deepest point in the Internet, and this layer contains the deepest sections of the dark web, and they will be able to provide confidential information and hidden services, and this level contains information about hacking programs and illegal data.[14]

Some deep sites are non-traditional markets offering an alarming array of products or services, where illicit drugs, weapons, counterfeit goods, stolen credit cards, hacked data, digital currencies, malware, national identity cards or passports can be purchased[15] or mediated.

The dark web includes a number of web pages that exist on the World Wide Web, these pages cannot be indexed by regular search engines, cannot be displayed in web pages, digital, or criminal services can also be contracted, ranging from spam campaigns to widespread denial-of-service (DDoS) attacks, and beginners can even buy e-books that explain how to attack sites, steal identities, or otherwise profit from illicit activities.[16]

The content of the deep web includes information in the form of a confidential database that can be accessed via the Internet, but not through search engines, but through a private IP address and secret accounts,[17] the dark web allows its users to maintain their privacy, in order to allow users to express themselves and their ideas freely without tracking them online, is the dark web the same as the deep internet? Approximately, 95% of the Internet is on the deep web, and popsci estimates the size of the dark web, five hundred times, what we see from the Internet, but this dark side of the Internet cannot be accessed in traditional ways, and dark web sites allow sending emails through special browsers such as the Tor browser and other browsers, and the "dark web" is one of the biggest challenges facing efforts to combat and confront takfiri and extremist groups, as it is a set of network links that use protocols other than (HTTP), but they exist on the public network, and are established in a closed and confidential manner between trusted parties between each other.[18]

---

[14] Mostafa Said, The Dark Web Decides Land of Hidden Terrorist Activities, "Excavations" is an electronic newspaper published by the Dal Center for Research and Media Production, Cairo, on 13/05/2018, available at https://www.hafryat.com/ar/blog/.

[15] Colleen McCue & Andre Parker, "Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis," Police Chief, 70, no. 10 2023.

[16] David Omand, Jamie Bartlett & Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", Intelligence and National Security 27, (2021).

[17] Ahmed Youssef El-Tahawy, Electronic Evidence and its Role in Criminal Evidence, Cairo, Dar Al-Nahda Al-Arabiya, 2015, pp. 21–23.

[18] Alaa Al-Attar, Study "Dark Depths... The Deep Network", National Center for Research and Opinion Poll, Damascus, Syria, Dar Al-Baath for Printing and Publishing, 2022, pp. 12, 13.

The "dark web" is also the main base for the launch of malicious attacks and DDoS, which now cost companies millions of dollars annually, from buying victims' data to exploiting them to extracting ransomware, noting that the competent authorities in countries allow the legal and normal use of virtual private networks «VPNs».» by companies, but prohibit the use of these private networks for the purpose of reducing the commission of crimes and access to prohibited information and other malicious activities that take place through the Tor network, with the aim of accessing illegal content, products or services is punishable by law in most countries, including the UAE, which allows the legal and normal use of virtual private networks «VPNs» by companies, but punishes the user with imprisonment and a fine for any prohibited activities in the dark web.

The difference between dark and deep web.[19]

Dark Web	Deep Web
The dark web is a subset of the deep web that is intentionally hidden.	The deep web is a layer of the Internet and does not appear from traditional search engines.
To access the dark web you need the Tor browser.	To access the deep web you need a password, special encryption or specialized software.
Sometimes used for illegal activities.	It is usually used for legitimate purposes that require anonymity.
It only includes a subset of web pages that are not indexed within the deep web.	Includes all non-indexed web pages.

Tor Engine Service and Deep Internet:
The term TOR is an acronym for The Onion Router, a multi-agent network that does not rely on specific proxy servers to process your data, but rather relies on the connections of many of its users, to hide the IP address of the original user, despite the risks surrounding the use of TOR. Like other proxy communications, it is an incognito browser for incognito access the Internet, developed by Roger Dingliden, Nick Matthewson, and Paul Severson and presented at the 13th Security Symposium of the Advanced Technical Computing Consortium on September 20,[20] 2002, and the stable version of the browser was released in 2009.[21]

[19] Masayuki, Deep web, Dark web, Dark net, Annals of Business Administrative Science, vol 19, 2020, page 285.

[20] 13th USENIX Security Symposium
https://www.usenix.org/legacy/events/sec04/tech/dingledine.html تاريخ 31/7/2022.

[21] Henry, S &W. Einstadter: "The criminology theory reader", New York, NY University Press, 2001.

Tor uses two channels in order to hide user activity on the network— the first is an encrypted channel to encrypt communication via TLS and the second is not encrypted known as the directory service and is used to find out where another Tor adapter is, while the blocking process is done by cutting any HTTP GET request to ₹, the Tor browser depends on The Onion Router technology, which is a system that enables users to connect to the Internet without revealing their identities, and in addition to the browser, the Tor project provides a number of applications that allow individuals and organizations to communicate and exchange information confidentially and securely to protect privacy and identities, so Tor is run through a group of devices called "nodes" chosen by Tor randomly to pass the connection and in each connection process there are three nodes, which are an entry node, a middle node, and an exit node, and this method prevents anyone from monitoring users' connection to the Internet, and also hides the geographical location of the user, and does not know which of the ₹services are used and access them when browsing.[22]

To understand the idea of onion routing, you must first understand the idea of direct routing used in the usual, used and common web around the world, as the usual web has a very simplified routing system, and when you need to access a specific web page, the computer or phone connected to the Internet sends the desired site address to dedicated servers bearing the name DNS and includes an archive of the addresses of the nominal sites (their links) and in return their actual addresses ((IP addresses).its own), and then the connection to the desired location becomes direct without really multiple stages.[23]

In the bulbar guidance system, things are clearly different in reality, as the information is sent to an independent party (another user of the dark web) first, where the receiver can read only part of the information, which is the address of the next station, while the content of the data remains encrypted, and here it is not done through one station only, but passes through many stations until it finally reaches the desired location, and upon return the information proceeds similarly and through a number of successive stages and stations until it reaches the user.[24]

What is distinctive about the bulbous guidance system is that each station along the route has a very small amount of information, as the transmitted information remains encrypted until it reaches the second end of the communication, and across stations each element in the chain knows nothing but the address of the next and previous stations, while the identity of the transmitter, receiver and the full path of the data remain completely anonymous.[25]

---

[22] Alaa Al-Attar, Study "Dark Depths... The Deep Web, op. cit., p. 16.

[23] Kingstone ali mwila. The deep web‹P.g degree. The university of zombia lusaka. page 3.

[24] Mushir Fayez Aziz: "Security Analysis and its Role in Predicting and Preventing Crime", PhD thesis, Faculty of Graduate Studies at the Police Academy, 2015, p. 199.

[25] Kristin Finklea, Dark Web, Congressional Research Service, informing the legislative Debat, 2017, page 12.

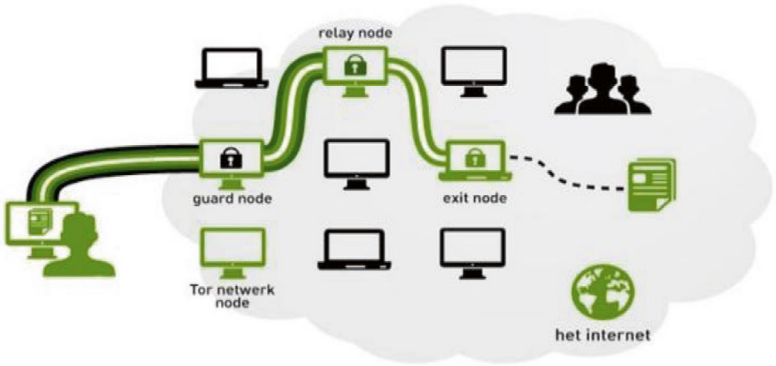


Fig. 2 Onion routing

- For example, suppose you live in Cairo and want to send a message to a friend in London, you can in principle include the message in an envelope bearing the address of your final future friend, but here anyone intercepting the message will be able to identify you as the sender and your London friend as the recipient of the message.[26]
- If you want to get more security for the message you send, you can rely on wrapping it in several postal envelopes in the form of successive layers, where the first circumstance refers to the address of a person in Baghdad, for example,[27] and there when the envelope is opened, the receiver in Baghdad resends the message to another address such as Al-Ain, and from there, it is sent to Vienna, then Khartoum, and finally London, for example, this way, anyone who sees the message on its way won't be able to know the sender's address or the final receiver, but only the address of the previous and next stop in the message journey. In principle, the transmitted information is covered by successive layers of forwarding and encryption, and because of the multiplicity of these layers, it is called onion routing because, like the bulb, it has many layers superimposed on top of each other, as shown in the Fig. 2.

Since the idea of the dark web began, the basis was privacy and maintaining the confidentiality of both the sender and the receiver is the basis, and relying on onion routing technology, this goal is fully achieved, as the large number of successive encryption and retransmission layers makes access to the content of the

[26] Ammar Yasser Al-Babli, Mechanisms of Artificial Intelligence in Confronting Violent Extremism, refereed research, Journal of Police and Legal Sciences, Academy of Police Sciences in Sharjah, Vol. 13—Issue 2—2023, p. 298.

[27] Shoaib Adam, President: "The security confrontation of the crime of electronic terrorism in the United Arab Emirates", op. cit., p. 297.

message almost impossible, and it also stands in the way of tracking communications to and from the sender and receiver, and with the path of communication between the two parties of the communication changing all the time, tracking becomes almost impossible.[28]

This important feature of the dark web makes it the place of choice for many types of illegal activity, and although it was not designed for criminal purposes but for the government use of the United States, it is available to everyone and is used for many criminal purposes today.[29]

Given what it provides GATE, which stands for "The Onion Router", multi-layered encryption of information and routes traffic across individual server sites, resulting in the generation of addresses IP Different for each operation, users must add an extra layer of protection by using a VPN.[30] ₹ is now used for illegal activities. This can include protecting privacy or circumventing censorship, as well as posting child abuse content, selling drugs, or distributing malware. According to one estimate in general, digitized currency Bitcoin (bitcoin), the currency used in the dark web is a site Silk Road[31] (a dark web site), as a "dark corner of the web". The "dark web" is also witnessing a great popularity of illegal activities that have been able to achieve millions' profits. These activities include human trafficking, drugs and weapons, various prostitution trade, purchase of illicit drugs, counterfeit goods, stolen credit cards, compromised data, digital currencies, malware, national identity cards or passports, including child prostitution, as well as the provision of the services of hither.

4 Crimes of Sexual Exploitation and Extortion of Children and Artificial Intelligence Mechanisms in Monitoring and Confrontation

Booting and Partitioning:
Child sexual harassment is increasingly emerging around the world, becoming a serious problem exacerbated by the rapid development of technology. Child

[28] Ahmed Youssef Al-Tahawy, Electronic Evidence and its Role in Criminal Evidence, previous reference, p. 28.

[29] Amany Al-Rayes: "Using Network Analysis Methodology in Studying Societal Trends on Social Networks—Applied to Assessing the Demand for Official and Private Media on Those Networks", Research Activities Bulletin, No. 14, Institute of National Planning, Cairo, 2017, p. 302.

[30] Information Commissioner's Office، Information Commissioner's Report to Parliament on the State of Surveillance (November 2019) pp. 98–100.

[31] The Silkroad website, founded by Ross Ulbricht in 2011, is the most famous and important deep web site, which was an e-commerce site, but not in the familiar sense of such sites, but Bruce traded in anything illegal, from the arms trade, all kinds of drugs and real estate, through the sex and organ trade, the trade in forged personal documents or false driver's licenses, credit cards, stolen goods, pirated software, money laundering, and others.

sexual abuse has become readily available online and without significant risk as a result of the use of true anonymity features. This situation prompted experts in this field to sound the alarm and seek effective solutions to confront this alarming phenomenon.

Based on this, experts have resorted to artificial intelligence techniques to detect and predict sexual abuse, with the aim of early intervention and limiting its spread. These experts are focusing their efforts on addressing this challenge, which has led to the transformation of child victims of sexual harassment from the real world to the virtual world, with their increasing physical and psychological impacts. It can process huge amounts of data quickly accurately, and can detect patterns and tags that are difficult to detect manually. AI can also provide objective and equitable analysis of available information, and help channel resources and prioritize.

Overall, joint efforts between AI and humans can be most effective in combating child sexual exploitation crimes. AI can provide powerful tools and analytics to humans, enabling them to make better decisions and achieve more effective outcomes in protecting children and providing justice to victims.

Experts also monitored an increase in the number of attempts to access illegal websites displaying child sexual abuse material. Production, access, and dissemination of child sexual abuse material directly on the Internet is now an easy alternative to luring children into sexual activities and selling images online.

97 million videos and images in 2023 of the rise in child pornography on the Internet and the harm to millions of children are devastating[32]

4.1 First Requirement

Online Child Sexual Exploitation and Extortion Crimes

Sexual crimes committed online have increased significantly, their forms have diversified, and their numbers have multiplied, seriously exacerbating this phenomenon. Criminals and sexually deviants benefit from the sophistication and ease of use of technology to spread their devious ideas and commit their crimes, especially with the high rate of computer and Internet use by children, making them an easy target for trolls and sexual perverts.[33]

Globally, countless young people are victims of sexual misconduct and exploitation. Such violations are widespread across all strata of society and States

[32] Human Rights Expert: New forms of child sexual abuse emerged after the COVID-19 pandemic, UN News, https://news.un.org/ar/story/2020/05/1054392.

[33] Dr. Imad Al-Fraihat, Mechanisms for combating the crime of electronic sexual exploitation of children in Jordanian law "a comparative study", Journal of Humanities and Natural Sciences, Ajloun National University, Amman, 2023, p. 22.
HNSJ, 2023, 4(5); https://doi.org/10.53796/hnsj4514.

and children, especially girls, are at high risk of forced sex, sexual exploitation, abuse and violence on the Internet.[34]

5 The Internet Contributes to Child Pornography

With the advent of the Internet and the rise in the number of users of social networking sites, the spread and circulation of these behaviors has increased, and their production has become easier and more diverse. As a result, what is known as digital forensics, which is used to investigate cases of child rape, has emerged. Studies have shown that the Internet contributes to the exploitation of children in pornography by increasing their possession, easy download, efficient, and accessible distribution. The Internet offers many advantages in this context, including,[35]

- *Access large amounts of pictures from all over the world.*
- *Pornography is available anytime, anywhere.*
- *Access content anonymously and confidentially.*
- *Facilitate direct communication and image exchange between users.*
- *Providing high-quality digital images and easy storage.*
- *Provide a variety of formats for pornography, including images, videos, audio, and virtual interactive experiences.*

6 Second: Sexual Exploitation of Children Through Internet Layers

According to the European Convention for the Protection of Children against Sexual Exploitation and Abuse, such exploitation can be divided into several different categories, one of which is sexual abuse, which includes any conduct involving sex with children, whether related to coercion, threats, breach of trust, abuse of authority, or the ability to co-opt the child[36].

[34] The role of the United Nations in protecting children from sexual blackmail: https://www.un.org/ar/observances/child-sexual-exploitation-prevention-and-healing-day.

[35] Amar Elbably, Combating the Exploitation of Children in Cyberspace: Technical Mechanisms to Protect Children From Sexual Content, Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities, 2021 IGI Global. https://www.igi-global.com/chapter/combating-the-exploitation-of-children-in-cyberspace/270488 (www.scopus.com).

[36] Dr. Hossam Nabil Al-Sharnaqi, International Cooperation in Combating the Sexual Exploitation of Children, Security and Law Magazine, Dubai Police Academy, First Issue, January 2020, p. 201. It is available on: https://dubaipolice.ac.ae/dpacademy/ar/sada_acadmey/show_doc.jsp?doc_type=sum_file&book_id=137.

In addition, the production and use of sexual images and clips that show children are other forms of sexual abuse for the purpose of achieving sexual, financial, or other benefits. The perpetrators of this type of crime can be adults or children themselves, and child sexual abuse material is often produced by tricking the victim into participating in the production of that pornography.

In the area of child rights studies and legal investigations of child sexual exploitation, child pornography is a complex and diverse phenomenon.[37]

The researcher believes that the pornography in the images varies greatly, as it can be divided into several levels ranging from guidance, nudes, erotica, pretense, sexual arousal, explicit sex, explicit sexual activity, assault, gross abuse, sadism or bestiality, exploitation of children in pornographic shows, spoiling children and luring children for sexual purposes.

7 Third: Rise of Victims of Sexual Exploitation of Children Online

The use of children in this pornography is a flagrant violation of their rights and puts them at great risk and the international community and legal authorities must take firm action to combat this heinous phenomenon, including tightening laws, raising public awareness, and strengthening Internet censorship.

For example, the number of children in the Philippines who were victims of sexual exploitation was *500,000 children in 2022, which is equivalent to one child per 100 children, part of it through video and live streaming platforms for financial and commercial gains in criminal organizations and mentally ill people. A report published by the We Protect Global Alliance revealed an 87 percent increase in cases of reported sexual abuse in children in 2023 compared to 2019. The number of cases has reached more than 32 million globally, according to the National Centre for Missing and Exploited Children*.[38]

The issue of online child exploitation and abuse continues to evolve as a complex and multidimensional issue. Since 2021, new trends have emerged in the harms caused by these crimes, while previous harms have continued without being adequately overcome. Photos and videos make up a large proportion of this type of assault. In 2022, the percentage of reports involving material suspected of being sexual abuse of children was more than 99.5% of the total reports received by the National Center for Children. Of the 88.3 million files submitted by e-services

[37] Dr. Hossam Nabil Al-Sharnaqi, op. cit.

[38] UK Safety Tech Sector: 2022 analysis (UK Government, 2023) 352. Accessed from: https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech/uk-safety-tech-sector-2022-analysis 18/08/2023.

companies in the same year, there were 49.4 million photos and 37.7 million suspected videos. The following analysis shows the current landscape of harms associated with the production, viewing, and sharing of child sexual abuse material, the techniques used, and the information available on perpetrators of abuse[39] offences.

The report, which provides an in-depth and fundamental look at the threats children face online in 2023, revealed a 360 percent rise in sexual images taken by children of themselves in the age group of 7 to 10 years between 2020 and 2022, according to the Internet Watch Foundation. While the overall average grooming time is only 45 min, group play environments that facilitate the mixing of adults and children, virtual gift exchanges, and public rating systems contribute to this risk significantly,[40] high.

In December 2023,—We Protect released its fourth Global Threat Assessment Report, which revealed an 87% increase in reported child sexual abuse cases since 2019, with more than 32 million reports globally (NCMEC).[41]

The findings underscore the urgent need for a coordinated and multifaceted response to protect the world's children from this escalating threat around the threats children face online in 2023, that there is a 360% increase in self-generated sexual images of children aged 7–10 years from 2020 to 2023 (Internet Watch Foundation). Shockingly, it has also been revealed that conversations with children on social gaming platforms can escalate into high-risk grooming situations within 19 s, with an average grooming time of just 45 min. Social gaming environments that facilitate mixing between adults and children, virtual gift exchanges and public rating systems, significantly increase these risks. The research found a significant rise in financial sexual blackmail, internet reporting has increased and this involves luring perpetrators and manipulating children to share sexual images and videos of themselves, and then blackmailing them for financial gain. Many blackmailers pretend to be young girls online and mostly approach boys between the ages of 15 and 17 via social media. This phenomenon has led to a series of cases in which children have tragically committed suicide.

[39] CyberTipline 2022 Report (National Center for Missing 1and Exploited Children, 2023) Accessed from: https://www.missingkids.org/cybertiplinedata 16/08/2023.

[40] WeProtect Global Alliance report, Global Threat Assessment, Assessment of the Scale of Child Sexual Exploitation and Abuse 2023 and available at: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-AR.pdf.

[41] https://www.weprotect.org/wp-content/uploads/Global-Threat-Asssesment-2023-Press-Release.pdf.

8 Fourth: Methods and Stages of Sexual Exploitation of Children via the Internet

1. Chat Rooms

Online chat rooms or chat rooms have become an important and popular tool in our time. However, their exploitation by unsafe people to lure and sexually exploit children online has become commonplace. This is due to the great popularity of these sites among children and adults, and to the various services they provide, where individuals can participate in multiple conversations in one framework or in multiple groups. With the advancement of communication technology, these conversations have evolved from written conversations to voice conversations, and then to video conversations, where parties can see each other using available cameras.

It is important to mention that conversations that take place in chat rooms can be documented, recorded, distributed, and maintained, and this increases their risk significantly, especially when used to blackmail victims. Given the ease of luring and rhythming children, this greatly increases the risk of these conversations.

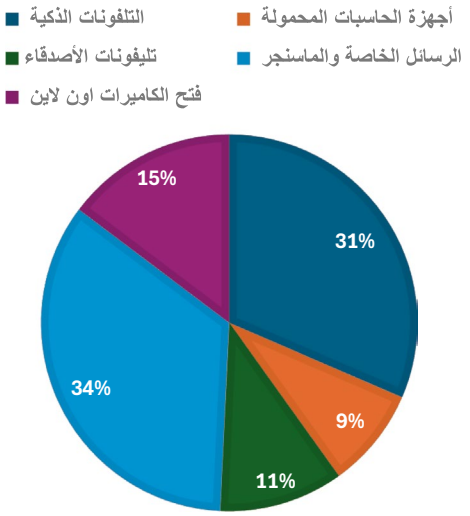
2. Stages of Child Sexual Exploitation Through the Internet and Dark Web:
   - Pornography production: At this stage, perpetrators create pornographic images, whether by editing existing images or recording new pornographic content in which children appear clearly and the perpetrators benefit from the rapid technological development, where they can produce high-quality photos and videos using digital cameras and advanced webcams and also use public places and social media to take photos without the children's knowledge.
   - Distribution of child pornography: This stage involves the dissemination of child pornography on the Internet and the perpetrators upload this material to site servers or use social media groups to request child pornography and these operations include the exchange of content via direct messages or chat and forums. The authorities monitor online activities and suspicious websites, so perpetrators use advanced techniques to maintain anonymity and avoid being identified.[42]
   - Download and upload child pornography: This stage is related to obtaining child pornography online, where perpetrators can access these images without the need to store them on their devices, and this is done via unsolicited email links or by accidentally going to pornographic sites, and perpetrators need advanced technical skills to search for and access these sites, and it may require paying fees or using passwords to access child pornography

[42] Dr. Hossam Nabil Al-Sharnaki, International Cooperation in Combating the Sexual Exploitation of Children, previous reference.

content. These criminal activities continue and require integrated efforts between legal entities, and Internet service providers to eliminate these crimes and protect children from exposure to them.

Offenders often produce cartoons with the aim of attracting children and making them victims of them. These pornographic cartoons include creative replicas and originals, as well as their use to pull images and drawings from sources as diverse as movie or magazine footage using a scanner.

They also perform digital manipulations such as montage, dubbing, and alteration, where they assemble pieces of different sexual images to create false scenes, such as fake rape scenes or superimposing images of known people on naked bodies. These images may include images of adults or children, and sometimes appear to be real. The perpetrators then turn to sexually exploit these images online, where the aim of the production is not just to create the images but to achieve the sexual exploitation of children through media.[43] Digital image illustrates access to child sexual abuse and the place to be seen and participate[44]:



Report reveals high risk of online child sexual exploitation and abuse.[45]

[43] Al-Qadhi, Mishaal bin Abdullah, (2015), Pornographic sites on the Internet and their impact on the individual and society, Saudi Arabia, Al-Minshawi Center for Studies and Research, p. 122.

[44] WeProtect Global Alliance report, Global Threat Assessment, Assessment of the Scale of Child Sexual Exploitation and Abuse 2023, op. cit., p. 27.

[45] https://arabic.cnn.com/science-and-health/article/2023/11/06/children-online-sexual-abuse-infographic.

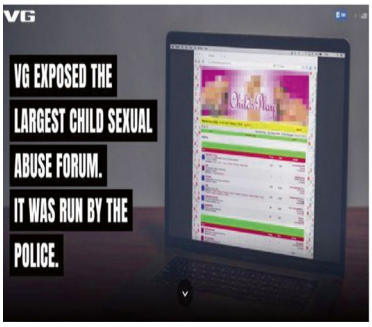
https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-AR.pdf.

Report of Child Sexual Abuse Material in 2023	32M
Increase the number of pornographic images and publications of child exploitation for the ages of 7-10 in 2021-2023	360%
of the cases of abuse was a known individual of the child	60%

I also find it alarming that this appears to be a case where showing the child's face is what lead to the conviction, unless I'm misunderstanding the story or something got lost in translation. They say that it happened at the same time they decided the girl lived in [redacted], so I don't know if that means they narrowed it down to the city and then checked social media photos, or if they identified her photo and also identified her location independently.

I have repeatedly told people that it's OK to show the child's face because you NEVER year of that being the factor that gets people caught. Producer shows a face – they're done. Show something that gives away your location? Done. But never based on just the girl's face.

From: Child sexual abuse material found on the dark webDarstellungen child sexual abuse on the darknet.





The figure illustrates the illegal child sexual exploitation websites.

Electronic extortion is a method of pressure and coercion resorted to by the offender to pressure the victim, and the blackmailer resorts in this case to threatening the victim with prejudice to his private life or defamation of him, and the crime of electronic extortion is based on the elements that must be available, the material element must be available, which is the activity issued by the blackmailer and has an external appearance through which he is known as well as the moral element must be available, which is the direct will of the offender. Criminal behavior is internal latent in the same offender, and I have taken the crime of electronic extortion has attracted a large part of the criminal legislator's attention after its widespread spread, and legislative efforts have accelerated to criminalize all forms of extortion, especially extortion through the Internet, and the Egyptian legislator did well by promulgating Law No. 175 of 2018 on combating information technology crimes.[46]

Also, a dangerous type of attacks and crimes that depend on advanced technologies (such as cloud computing, artificial intelligence, and the Internet of

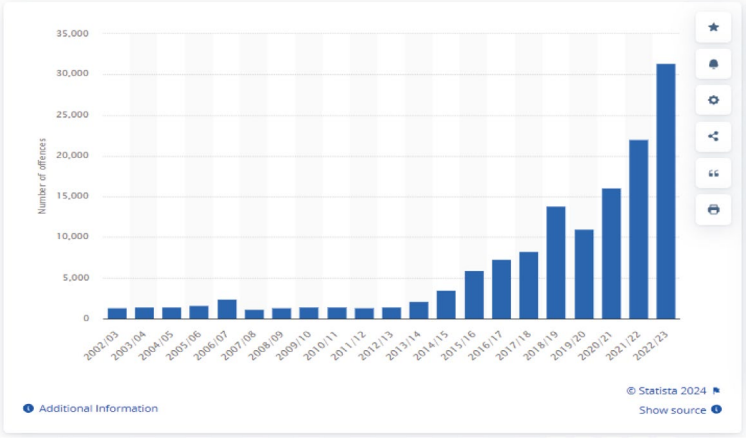
[46] Official Gazette, No. 32 bis (c), 14 August 2018.

Things), listening devices on communication networks, software to encrypt suspicious operations, and malicious software to penetrate network and computer security systems, to be harnessed to carry out criminal operations and suspicious transactions without the knowledge of their owners in so-called automated networks, where one automated network can include tens, hundreds of thousands, or millions of computers or devices connected to the Internet, which can be used to launch various attacks, such as attacks distributed to disrupt services on targeted networks and sites for criminal purposes such as sabotage, terrorism, threats, and extortion.[47]

The statistics we study reveal important insights into the evolving cyber threat landscape. It highlights a critical fact: cybercriminals are diversifying their tactics, and no sector remains unscathed. The projected staggering rise in cybercrime costs to $10.5 trillion by 2025 reflects the increasingly bold and sophisticated attacks are incredibly.

The[48] Optional Protocol to the Convention on the Elimination and sexual blackmail crimes.

Figure showing the rise in electronic and sexual blackmail crimes against children and women.



In light of the continuous technological development, cyber extortion has become a challenge that poses a threat to individuals and institutions in Egypt.

Electronic extortion is defined as the use of technology to threaten individuals with the disclosure of sensitive information or obtaining illegal gains, as it is

[47] Hisham Mohamed Farid Rostom, Penal Code and Information Technology Risks, Modern Machines Library, Assiut, 0p. 1.

[48] https://www.cobalt.io/blog/cybersecurity-statistics-2024.

the process of threatening and intimidating the victim by publishing photos or film materials or leaking confidential information about the victim, in exchange for paying sums of money or exploiting the victim to carry out illegal acts for the benefit of blackmailers, such as disclosing confidential information about the employer or other illegal acts.

Victims are usually phished through e-mail or various social media such as Facebook, X "Twitter previously", Instagram, and other social media due to their wide spread and great use by all segments of society and the increase in electronic extortion, in light of the growing number of social media users, and the acceleration witnessed in the number of various chat programs.

Within the framework of Egyptian law, these acts are punished under specific articles, as Article 308 of the Penal Code provides for severe penalties of up to imprisonment when it is proven that they are involved in acts of threat or extortion through electronic means, and this aims to protect citizens and ensure the security of personal information of individuals, and the Egyptian Penal Code stipulates in Article 327 that "Anyone who threatens another in writing to commit a crime against himself or money is punishable by death" or hard labor for life or temporary, or by disclosure of matters or attribution of matters that offend honor, shall be punished by imprisonment and reduced to imprisonment if the threat is not accompanied by a material request".

Threatening one person to another with a crime against oneself carries a penalty of imprisonment for a period not exceeding 3 years, if the threat is not accompanied by a request for money, but if it is accompanied by a request for money, the penalty may reach 7 years in prison.

Article 25 of the Anti-Cyber and Information Technology Crimes Law stipulates that anyone who violates any of the family principles or values in Egyptian society, violates the sanctity of private life, sends many e-mails to a specific person without his consent, or grants personal data to a system or website to promote goods, shall be punished by imprisonment for a period of not less than six months, and a fine of not less than fifty thousand pounds and not exceeding one hundred thousand pounds, or by one of these two penalties, or services without his consent.

It stresses the importance of reporting cases of electronic extortion to enable the competent authorities to take the necessary measures, and individuals must commit to directing complaints to the concerned authorities, and cooperating with investigations to ensure that those involved are held accountable.

It is worth noting the importance of raising awareness about the danger of electronic extortion and how to avoid it, as digital transformation plays a vital role in promoting awareness among individuals and society.

As the Crime of the Shubra Child

In order to covet the millions of pounds he will receive after carrying out his crime and documenting it by publishing the clip on "The Dark Web" and selling it to the human organ trade mafia, the crime known in the media as the crime of the Shubra

child, which was the instigator in Kuwait and the killer and victim in Egypt, took place.[49]

The dark web is a small and obscure part of the Internet, unavailable via traditional search engines, requiring special techniques to access it, and is notorious for its secret browsing and use in illegal activities.

Kaspersky Lab, a Russian company specializing in designing anti-virus software, defines the "dark web", or what is also called "dark web", as the secret web that consists of a group of websites hidden from the eyes of followers.

The company adds: The hidden and dark part of the Internet, and difficult to access the dark web, is easily accessible through the traditional search engines available.

The dark web represents a great danger to the minds of children and adolescents, as through the Internet site «dark web» various secret business transactions, and can be navigated and roamed in its sites without the person leaving any traces, that is, he will be anonymous, and his activities are not registered on any search engines, and cannot be tracked.

9 How Did the Shubra Child Crime Occur?

According to the statement published by the Public Prosecution about the crime of the Shubra child, the perpetrator confessed that the crime was instigated by an Egyptian citizen residing in Kuwait—who was deported to Egypt and arrested—who confirmed that its purpose was to sell and publish it through websites broadcast in exchange for «large sums of money».

She confirmed that the accused, after he carried out what was asked of him, assigned him to an Egyptian resident in Kuwait to repeat the matter with another child to get the agreed amount, but he was caught before doing so, and the Public Prosecution did not find any medical equipment that indicates that what is meant is the trade in human organs.

[49] The events of the Shubra child crime took place between Kuwait and Egypt, and the 15-year-old Ahmed Saad who lives in Ezbet Othman in Shubra Al-Kheima in Qalyubia Governorate.

The Shubra child was not the first victim, who kills and steals his organs through the so-called dark web, as he was a victim of a gang working in organ trading through «video call» between them, and selling the crime video for large sums.

The killer filmed the crime "live" online, cutting off the victim's organs, to facilitate their sale to the organ trafficking mafia via the Internet "dark web".

The "Shubra Crime" raised questions about "The Dark Web", which the Kuwait-based instigator of the murder of the victim stated that he would publish the video of the incident via the "Dark Web", to facilitate the sale of the clip to the "organ trade mafia".

The investigations confirmed that the goal of the Shubra child crime was not organ trafficking, but the sale of the crime video for astronomical sums through illegal Internet sites «DrakeWeb».[50]

10 Details of the Crime of the Shubra Child

The investigations revealed that the victim was found dead, in a rented apartment, in the Shubra al-Kheima area, (north of Cairo), and next to his body a bag containing a number of organs, and showed that the defendants, the first who resides in the child's residential area, have a prior relationship with the second defendant, who was residing in Kuwait, and Egypt received him, from the Kuwaiti authorities, in accordance with the agreements between the two countries.

The investigations showed that the father of the second defendant was summoned (since the phone line used in his name), but he denied that he had anything to do with the incident, and said that he did not know that his son instigated the killing of the child this time, or on previous occasions.

The investigations, in the case No. (1820 of 2024—Administrative First Department of Shubra Al-Kheima), proved the confessions of the second defendant, the "instigating party", that he communicates from Kuwait with the actor party, and that he was asked to carry out a new killing operation, and that the execution be (live) over the phone, which is what actually happened, in order to broadcast it and obtain opportunities to sell organs, and make large profits, as the first defendant confessed, that he agreed to obtain 5 million pounds, in exchange for carrying out the operation.

The security investigations indicated that the killer's neighbors never suspected him, and indicated that he has been living in the area for a while, and that he rumored among them that he is a "tumor patient", and that he regularly prays in

[50]The prosecution continued in its statement: «The investigations resulted in the knowledge of the Egyptian defendant residing in Kuwait, who used in committing (the crime) a mobile phone equipped with a SIM card owned by his father, and based on the instructions of the Attorney General's Counsel, the Department of International Cooperation at the Attorney General's Office contacted the competent authorities in the State of Kuwait, and the International Interpol, which resulted in the seizure of the accused and his father, and their possession of electronic devices, as they were deported to Egypt, so the Public Prosecution began interrogating them up to the reasons for committing the crime».

It stated that «the first defendant, who exceeded the age of fifteen, admitted that he was the one who instructed the perpetrator of the crime to commit it, as stated in his acknowledgment, intending to keep the video clips of the killing of the child victim and the mutilation of his body, so that he had the opportunity to sell and publish them through the websites that broadcast them in exchange for large sums of money, and he also decided that he had already done this act in previous times, and the validity of this is being verified by examining the defendant's electronic devices, and his father, who was caught with him and denied any connection to these incidents, and investigations are being completed."

the mosque of the region, and his relationship is good with neighbors, but in the recent period his financial conditions have changed, and he has recovered a lot, and he does not depend on the help of neighbors, and his clothes have changed, and it was rumored that his brother resides in Kuwait, who sends him money in the recent period.

It was also noted that he is approaching the children and youth of the region, and it was exposed with the disappearance of Ahmed, , a child of the crime a child of the crime of Shubra suddenly from the area, until his neighbor informed the parents, that she smells a foul smell coming out of his apartment on Thursday evening, at the time when the victim's family informed the police that her son disappeared, and here the crime was revealed, on Friday.

10.1 Dark Web Hazards

It is worth noting that dark web poses a danger to children for many reasons, including:

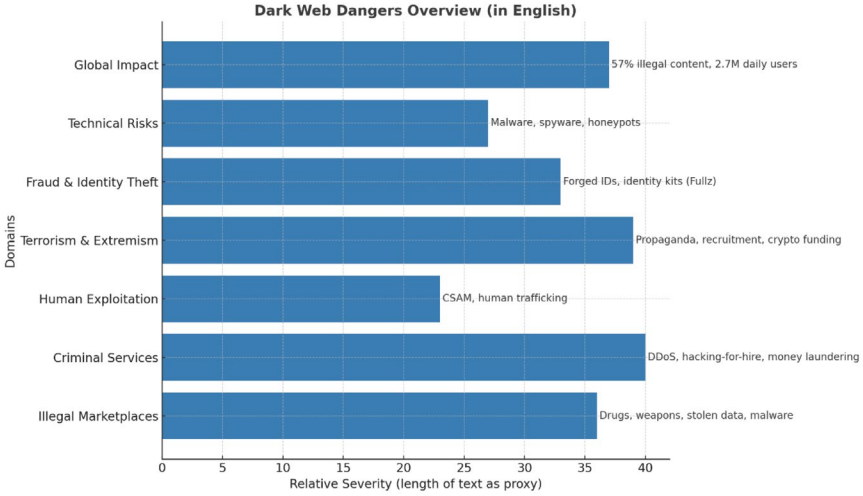
- Curiosity: Children are curious about exploring the virtual world, which can lead them to enter the "dark web" without realizing its dangers.
- Lack of awareness: Many children lack sufficient awareness of the dangers of the "dark web" and how to protect themselves from it.
- Accessibility: The dark web is more accessible than ever, increasing the likelihood that children will be exposed to it.

Children can be protected from the dangers of dark web by communicating with them on an ongoing basis, setting clear rules, and using parental control programs.

The dark web represents one of the most dangerous corners of the internet, hidden behind encryption networks like Tor and I2P. While not all activity there is illegal, it has become a hotspot for serious cybercrime and security threats. Here are the key dangers:

Domain	Main Risks	Examples & Impacts
Illegal Marketplaces	–Trade in drugs & weapons—Sale of stolen data—Distribution of malware	–Platforms similar to *Silk Road*—Sale of hacked bank accounts & crypto wallets
Criminal Services	–DDoS attacks for hire—Hacking-for-hire—Money laundering via cryptocurrencies	–Renting *Botnets*—Using *Mixers/Tumblers* to hide illicit funds
Human Exploitation	–Child Sexual Abuse Material (CSAM)—Human trafficking & smuggling	–Forums for illegal content sharing—Networks for migrant smuggling & forced labor
Terrorism & Extremism	–Propaganda dissemination–Recruitment & secret communication—Terror funding via crypto	–Terrorist propaganda channels—Encrypted chat rooms for attack planning

Domain	Main Risks	Examples & Impacts
Fraud & Identity Theft	–Forged documents (passports, IDs)–Complete identity kits "Fullz" for financial fraud	–Using stolen identities to open bank accounts or commit financial crimes
Technical Risks	–Malware & spyware—Websites infected with viruses—Law enforcement *honeypots*	–Devices infected with ransomware—Falling into digital traps of authorities
Global Impact	–57% of dark web content is illegal—Over 2.7 million daily users (2025)	–Direct threat to national security—Rising financial & social losses



11 The Role of Artificial Intelligence in Confronting Sexual Exploitation and Blackmail of Children

Artificial intelligence (AI) is a powerful tool that can be used to combat the sexual exploitation and extortion of children. The smart technologies and massive analytics provided by AI contribute to identifying patterns and behaviors associated with the sexual exploitation and blackmail of children online. By monitoring online activities and analyzing big data, AI can detect abnormal activities and suspect activities that may be harmful to children. Moreover, AI can be used to develop learning tools. A machine that learns from data and identifies normal and unusual patterns of online behavior, enabling the ability to detect and report on child sexual exploitation-like activities in a timely and effective manner.

In addition, AI can also be used to develop filtering and surveillance systems that help prevent access to harmful websites and content on the Internet, thereby reducing the chances of exploitation and sexual blackmail of children.

In general, artificial intelligence can be said to play an important role in combating online child sexual exploitation and blackmail, by developing analysis, monitoring and filtering tools that help effectively identify and prevent harmful activities.

First: The use of artificial neural networks in combating crimes of sexual exploitation of children:

How to use artificial intelligence techniques in combating child sexual exploitation crimes:

- Photo and video analysis: The use of artificial intelligence techniques in the analysis of images and videos makes it possible to identify pornographic content involving children by training the system on a large set of images to learn to distinguish between safe and harmful content, and then neural networks track the source of the film material, track and monitor IP and report it to the authorities, security services and technology companies.[51]
- Online behavior analysis: AI allows monitoring users' online behavior and detecting suspicious patterns. For example, changes in search pattern or interaction on social media that may indicate suspicious activity can be detected.
- Use of neural network techniques: Depth is used in data analysis using deep neural networks, which enhances the system's ability to identify complex and sophisticated patterns of sexual exploitation crimes and analyze images and videos and the pattern of those sites and groups.
- Identity disclosure: AI techniques can be used to verify the identity of persons suspected of or engaged in illegal sexual activity, whether online or in any other activity, thereby alerting or informing security and law enforcement authorities and[52] agencies.
- Web content monitoring: Technologies scan content across the web, including pornographic forums and sites, for any activity related to child sexual exploitation crimes. Algorithms and artificial neural networks can analyze text related to human trafficking crimes, such as illegal advertising, emails, or social media conversations to identify patterns and keywords that indicate the presence of crimes. Algorithms and artificial neural networks can also be used to analyze images and videos to determine Signs of exploitation, physical abuse, and identification of people involved

[51] Sarah Brayne. 2020. Predict and surveil: Data, discretion, and the future of policing. Oxford University Press, USA.

[52] Angus Crawford and Tony Smith, How AI is Used to Traffic Child Sexual Abuse Images, BBC International report of 28 June 2023 and available at:
https://www.bbc.com/arabic/articles/clwd844084xo.

- Cooperation with ISPs[53]: Collaboration with ISPs is underway to identify and report child pornography content and block such sites from key servers and prevent them from reaching families, children and communities.
- Privacy and data protection: Great attention is paid to protecting the privacy of users during the collection and analysis of data, and encryption techniques are used and other security means to maintain the confidentiality of information.
- Text analysis and content analysis: Text analysis is used to monitor online textual content, such as conversations and comments, to detect any content that indicates illegal activities.
- Cooperation with enforcement authorities: Integration with enforcement systems allows specific and effective efforts to be directed to combat sexual crimes against children.
- Temporal data analysis: Data can be analyzed over time to monitor changes in behavior patterns and discover new trends in sexual exploitation crimes.

By using these techniques in an integrated manner, the capacity to monitor and combat crimes of sexual exploitation of children can be strengthened, and to achieve greater efficiency and effectiveness in protecting and responding to this dangerous phenomenon.

Second: Enhancing Cybersecurity Using Artificial Intelligence:
The use of technology and artificial intelligence in cybersecurity has many potential advantages and benefits, and artificial intelligence can contribute to mitigating cyber threats and increasing the effectiveness of response to them through[54]:

- Threat detection and prevention: AI can analyze network traffic behavior and identify abnormal patterns that indicate cyberattacks. This allows organizations to take proactive measures to reduce the chances of breaches.
- Rapid incident response: When an attack occurs, AI can analyze the attack and identify affected systems, helping to provide immediate remediation strategies and minimize the impact of the attack.
- Predictive analytics: By analyzing current data and trends, AI can help organizations anticipate potential threats and take preventive measures before an attack occurs.

[53] Within the alliance, large companies such as Snap, Discord and Mega meet, the latter being a New Zealand platform with a particular focus on privacy, come together. In the context of the coalition's efforts, a pilot version of the program succeeded in removing more than ten thousand personal Facebook accounts, pages and Instagram accounts in cooperation with Mega, where it shared a set of data. To enhance digital security, Meta reported the accounts in question to the U.S.-based National Center for Missing and Exploited Children. has also shared the findings with other platforms to facilitate their own investigations.

[54] Tu, C.Z.; Yuan, Y.; Archer, N.; Connelly, C.E. Strategic value alignment for information security management: A critical success factor analysis. Inf. Compute. Secure. 2018, 26, 150–170. www.scopus.com

- Collaboration and partnerships: Collaboration between the public and private sectors and research institutions is crucial to address advanced cyber threats. The exchange of information and experiences contributes to enhancing cybersecurity.
- Education and training: As the field of artificial intelligence evolves, skills must be developed and continuous training provided to cybersecurity teams. This allows them to make the best use of new technologies.

Artificial intelligence can help educate children about online safety as follows:

- Educational apps and games: Educational apps and games can be developed that use artificial intelligence techniques to educate children about online safety. These apps and games can provide interactive and educational content that explains the potential risks and provides tips and guidance to children on how to keep them safe and private online.
- Smart interfaces: Smart interfaces can be developed that use artificial intelligence techniques to provide guidance and guidance to children while they browse the Internet. These interfaces can detect harmful or inappropriate content and provide instant alerts and guidance to children to help avoid risks.
- Smart voice assistants: Smart voice assistants such as AI assistants (such as Alexa and Google Assistant) can be developed to provide tips and guidance to children on online safety. These voice assistants can respond to children's questions and provide tips on how to handle online content and interactions safely.
- Analysis of children's online behavior: AI can be used to analyze children's online behavior and provide specific reports and recommendations to parents and educators. These reports can highlight unsafe or suspicious activities and provide guidance for improving children's online behavior.
- Analysis of interactions and content: AI techniques can be used to analyze the interactions that children make online and monitor the content they interact with. Through this, AI can identify potential lures and provide warnings and guidance to children on how to deal with them and stay away from them.
- Machine learning to detect psychological manipulation: Machine learning models can be trained to recognize the psychological manipulation tactics exploiters use to lure and lure children. These models can analyze messages and conversations and warn children when grooming attempts are suspected.
- Monitoring hazardous activities: AI can monitor and analyze children's online activity to detect risky behavior patterns. For example, if AI detects that a child is interacting with a stranger trying to obtain personal information or making inappropriate presentations, it can guide the child and provide warnings about the potential danger.
- Help filter out fraudulent messages: AI can analyze emails and chat messages and identify fraudulent messages and solicitations. This analysis can filter out malicious messages and prevent children from interacting with them.
- Using these technologies, AI can enhance children's awareness about online safety and equip them with the knowledge and skills to tackle potential risks.

Third: The Role of Technology Companies in Monitoring Child Pornography Platforms:

- Apple announced a new system that allows the monitoring of material related to child sexual abuse (CSAM) in iPhone devices and the system allows searching for CSAM materials before storing images on the iCloud Photos system, and in the case of a match, a human reviewer evaluates the content and reports it to law enforcement authorities, and despite concerns about privacy violation, Apple confirmed that the system achieves high accuracy and an error rate of less than one trillion per year, and Apple will manually review the conformity detection reports and if confirmed, action will be taken to disable the user's account and report it to the authorities, with the company emphasizing the benefits of this technology in terms of privacy based on the system's learning from users' images to detect the presence of CSAM material in their accounts.[55]
- It is worth noting that the European Union: has prepared a new application "Protech" aimed at reducing the viewing of child sexual abuse material online, with funding of $ 2.17 million from the European Union, this application will be tested by volunteers who have asked for help to resist their desire to see images of child sexual abuse, and the new application will be installed on devices such as mobile phones, where it will identify abusive images and videos and prevent them from displaying. It is hoped that this application will play a role in combating the "growing demand" for child sexual abuse imagery.[56]
- Databases should be created to identify suspected sexual harassers: AI can be used to create databases containing information about known and suspected sexual harassers. These rules can be used to detect people attempting to exploit children online and provide warning and prevention mechanisms.
- Companies are very keen to combat child sexual exploitation online, and we invest heavily in using technology to monitor and prevent the publication of this type of content on all of our platforms. Our efforts include advanced software monitoring and reviews by specialized teams, as well as reports from users and third parties, such as non-governmental organizations. We use hash matching and YouTube's CSAI Match, to monitor known material containing child sexual abuse. We also rely on classification tools based on machine learning technology to detect child sexual abuse material that has not been previously detected, and verified by specialized review teams. Monitoring previously undetected child sexual abuse material contributes to the integrated child safety ecosystem

[55] James Clayton, Apple to scan iPhones for any child sexually abusive content, BBC International report dated 6 August 2022 available at: https://www.bbc.com/arabic/science-and-tech-58086401.

[56] Chris Vallance, Child Sexual Abuse Image Ban App Funded by the European Union, BBC International report of 23 February 2023 available at: https://www.bbc.com/arabic/science-and-tech-64734567.

in several ways, including identifying victims in need of protection, and contributing to improving the retail match collection to enhance our ability to monitor known child sexual abuse material. Through the use of rating tools, Google has developed the Content Safety API that it provides to qualified parties to help them prioritize offensive content for review by professionals.

- Google's child safety team is developing technologies to effectively detect and report child sexual abuse material, to protect users and prevent physical abuse of children on Google platforms. We have developed a comprehensive set of child safety tools to ensure that these effective technologies are available to the widest possible base of users, and to contribute to preventing the spread of child sexual abuse content online.
- In addition, we are introducing Google's Hash Matching API to the NCMEC hub to help it process and review CyberTipline reports more efficiently, allowing them to focus on cases that require immediate intervention.
- We also work on sharing references related to sexual abuse and exploitation of children, enabling us to better remove this content from our platforms and through collaboration with NCMEC, we share millions of hashtags related to child sexual abuse. Thus, other providers can access and use these tags.
- In addition, we participate in Project Lantern, an initiative that aims to provide a safe and responsible way for technology companies to share information relevant to combating online sexual exploitation and abuse.
- By joining several consortiums, such as the Technology Coalition, WeProtect Global Alliance and HOPE, we are actively developing solutions to address the online sharing of child sexual abuse content and reduce child sexual exploitation, and we place these efforts as a top priority. In addition, we collaborate with NGOs such as NCMEC and Thorn to share knowledge, explore best practices, and address challenges related to child safety.

Digital forensics using artificial intelligence can help deliver justice in rape cases. Digital forensics is a branch of forensics that uses digital technology and electronic evidence in collecting and analyzing evidence in cases of rape and sexual assault crimes. Digital forensics is used to analyze digital evidence such as photos, videos, electronic conversations, digital records, and other data that can support the investigation of rape cases.

Digital analysis is used to determine the authenticity or falsification of digital evidence presented as part of an investigation, such as determining the source and timing of images and identifying their manipulation. Digital analysis may also be used to provide evidence of sexual assault, such as analyzing sexual images or videos to determine the existence of coercive measures or prove the occurrence of the assault.

Using digital technologies and tools, digital forensics can contribute to providing strong and credible evidence to courts, prosecutions, judges, and lawyers to deliver justice in rape cases. Digital forensics helps achieve justice by providing robust, scientific, and credible evidence to support those affected by sexual crimes and to investigate the conviction and justice of perpetrators.

- In 2023, the European Union created a new app aimed at reducing viewing of child sexual abuse material online, with funding of $2.17 million from the European Union.[57]
- The app, called Salus, aims to work in real time, using artificial intelligence to identify potential child sexual abuse material and prevent users from seeing it. The app will also use other traditional techniques to block content and help Internet Watch, an organization that searches, identifies, and removes child abuse material, train AI technology developed by Britain's Safe to Net.
- Facebook is developing new tools using artificial intelligence to limit searches for images and videos that contain child sexual abuse and prevent the sharing of such content. The move comes as the social network faces more pressure to combat the issue amid its plans to enable default encryption of messages on Facebook Messenger and photo service Instagram Owned by Facebook. End-to-end encryption means that except for the sender and recipient, not everyone can see messages, including Facebook and law enforcement officials.[58]
- The pop-up notification tool is the first Facebook has tested, as the notification appears when searching for terms related to child sexual abuse. The notice asks users to consider continuing the search and provides a link to transformer organizations, emphasizing the illegality of child sexual abuse and warning them of consequences including imprisonment.
- Facebook users who try to search for words related to child sexual abuse content receive this pop-up notification urging them not to view these images and get help. In 2023, Facebook confirmed that more than 90% of the content reported to the National Center for Missing and Exploited Children was identical or similar to the previous content.
- The second tool Facebook is testing is the Security Alert, where users are notified if they try to share these malicious images, with a warning that their accounts will be disabled. This tool is used to identify "behavioral cues" for users who may be more willing to share this malicious content.
- In addition, Facebook has updated its child safety policies and reporting tools, retracting content that shows children in inappropriate ways, and offering users an option to report suspicious content. Cases of child sexual abuse images have increased online during the coronavirus pandemic, with Facebook detecting at least 13 million harmful images on the main social network and Instagram during the period from July to September 2021.

[57] Chris Vallance, Child Sexual Abuse Photo Ban App Gets EU Funded, BBC Arabic, 23 February 2023 and available at: https://bbc.com/arabic/science-and-tech-64734567.

[58] Europol (2023) Child sexual exploitation. https://www.europol.europa.

Fourth: Security Confrontation of Crimes of Child Sexual Extortion via the Internet:

On the Security Side:

- Cooperating with telecommunications companies and local Internet service providers to provide the unit with all the technical information it needs, which is for the exploiter, such as the digital protocol address (IP Address), as well as the personal information registered with them such as his full name and address, which is information that is used to identify the owner of the account used in committing the crime. Locate him after the process of collecting technical and personal information and identifying the perpetrator, the location of the offender is determined either by the address registered with the telecommunications company that provides him with Internet service, or by GPS. After that, the offender is ambushed and seized, and the electronic devices he used in the crime are seized by legal means, after which the normal investigative procedures with the offender begin, and all the seized electronic devices are transferred to the digital evidence laboratory located in the unit, to be examined by specialized modern devices that reveal all their contents, whether they are still installed on them or have been deleted.

In 2021, four people were arrested in a multi-agency operation organized by a German investigation into one of Europe's most prevalent child sexual abuse platforms on the dark web.[59]

The dark web platform, known as Boystown, was removed by an international task force that included the German Federal Criminal Police (Bundeskriminalamt), and included Europol and law enforcement agencies from the Netherlands, Sweden, Australia, Canada, and the United States. The focus of this site was on child sexual abuse, and it had 400,000 registered users when it was removed. Several other dark online chat sites used by perpetrators of child sex crimes have also been seized in the same occasion.

This case illustrates what Europol sees in child sexual abuse crimes: online communities of perpetrators on the dark web show great resilience in adapting to law enforcement actions targeting them, and their reactions include reviving old societies, creating new communities, and making strong efforts to regulate and manage them. The photo and video data obtained during this investigation will be used in the victim identification task forces organized by Europol on a regular basis. More are expected to happen. Arrests and rescues are global, with police around the world examining intelligence packages collected by Europol.

The following participated in this investigation:

- Germany: Federal Criminal Police.
- Netherlands: National Police (politics).
- Sweden: National Police.

[59] Europol: https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users.

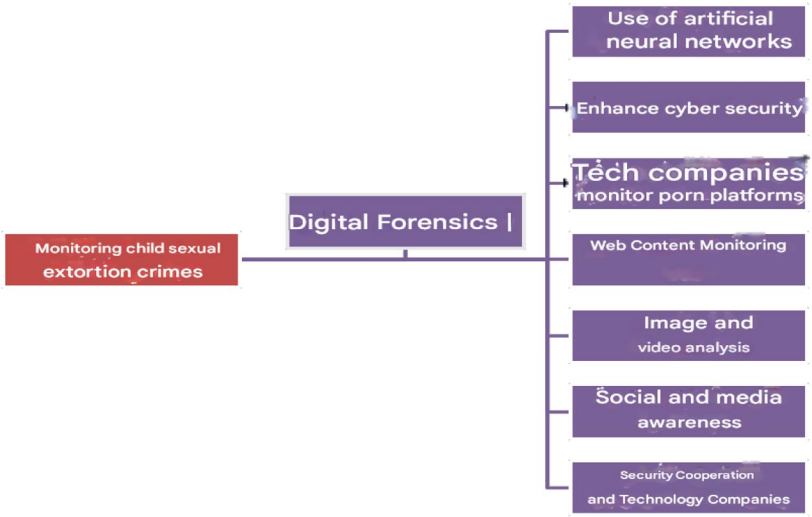
- Australia: Australian Child Exploitation Centre (ACCCE), Australian Federal Police (AFP), and Queensland Police Service (QPS).
- United States: Federal Bureau of Investigation (FBI) and U.S. Immigration and Customs Enforcement (ICE).
- Canada: Royal Canadian Mounted Police.

Fifth: Media and Societal Confrontation of Dark Web Crimes Through the Media: Raising public awareness and providing correct information about the crimes of human trafficking, smuggling of migrants, money laundering, sexual exploitation of children, and phishing are important aspects of efforts to combat these criminal phenomena other than combating terrorism and digital extremism. Law, media institutions, non-governmental organizations, Governments, and civil society[60] awareness-raising and education efforts must be continuous and continuous to raise awareness and enhance the ability to identify such crimes and work to prevent and combat them effectively.

- Societies today face enormous challenges resulting from the great danger that malicious websites pose to the social environment. This challenge begs the vital question: Where do we start? Because tackling these criminal groups must be a joint effort, governments and security actors cannot overcome this threat alone. Instead, there must be genuine cooperation between all human rights institutions, as well as educational institutions and journalism.
- Educational and awareness institutions are essential in this context, as they must direct their efforts towards spreading awareness among young people and enhancing their understanding of the dangers of these harmful gangs, and families must play an important role in transmitting this awareness to young people, and promoting the values of integrity and ethics to immunize them against the danger of these satanic groups.
- The role played by educational institutions, awareness, and families is critical in facing this global challenge. The dark web is a source of serious threats to individuals and families, so communities must work in harmony to preserve their values and principles, and to maintain their stability and safety.
- Provide comprehensive education about internet safety, including the risks associated with the dark web, how to recognize and avoid them, and encourage open communication between parents, educators, and young people to discuss online activities and potential risks.
- Promote the use of safe and reliable online browsing tools and teach young people how to identify and avoid suspicious sites.
- Organizing workshops, lectures, and awareness campaigns to educate young people about the potential legal, psychological, and security risks associated with accessing the dark web.

[60] Cyber Safety Prevention, presented by the Qatari Ministry of Interior during the Council of Arab Interior Ministers, on January 28, 2023 and available at: https://www.aim-council.org/awareness-programs/cybercrime-posters/49518/.

- Collaborate with regulators and information security experts to provide insights into real-life outcomes of interacting with the dark web while emphasizing the importance of using the Internet ethically and responsibly, and encouraging young people to report any suspicious online activities to trusted adults or authorities.[61]
- Providing awareness courses and workshops on digital safety and how to prevent the dangers of the dark web, conducting awareness campaigns through social media and public announcements to spread awareness about these risks, and organizing educational lectures in schools and universities to explain the potential dangers of using the dark internet and how to protect against them.
- Support programs to protect children and youth from harmful content and exploitation on the Internet while encouraging public debate and the media to shed light on cases of cybercrime and its harms.
- Promote a culture of staying away from illegal activities online and promote awareness of legal responsibility.
- Technology development and digital security: Advanced digital security technologies and tools must be developed to prevent and detect malicious activities on the Internet. The necessary tools for personal protection, encryption, and threat detection must be in place.
- Continuous training and education: Continuous training should be provided to individuals and organizations to enhance awareness and knowledge of the latest threats and technologies used in dark web crimes. Workshops and training courses can be organized for individuals and organizations to increase the level of digital security.



[61] Europol (2023) Internet organized crime threat assessment (IOCTA). https://www.europol.europa.eu/publications-events/main-reports/iocta-report. Accessed 12 march 2024.

Sixth: Awareness Mechanisms for Law Enforcement and Media Institutions for Crimes of Sexual Extortion, Electronic Harassment of Children and Sexual Exploitation of Children:

Raising public awareness and promoting awareness of crimes of sexual blackmail, online child harassment and child sexual exploitation are vital to reducing these crimes and protecting children. There are several awareness mechanisms that can be used by law enforcement and media organizations to achieve this goal, including:

- Public awareness campaigns: Public awareness campaigns can be organized on a large scale to raise awareness of crimes of sexual blackmail, online harassment of children, and sexual exploitation of children. Various media such as television, radio, newspapers, and social media are used to spread awareness messages and provide important information to the public and these campaigns should focus on informing the public about the types of crimes, their symptoms and tips to protect children.[62]
- Education in schools: Awareness topics on crimes of sexual extortion, electronic harassment of children, and child sexual exploitation can be included in school curricula. Children and adolescents are provided with the necessary information about potential dangers and how to self-protect and report any suspected cases. Teachers and student counselors should be trained to provide children with appropriate support and guidance.[63]
- Media role: Media organizations play an important role in disseminating news and reports related to crimes of sexual blackmail, electronic harassment of children, and sexual exploitation of children. Issues related to these crimes are highlighted and important information is provided and clarification is provided to the public about the causes, effects, and measures that can be taken to combat them. These institutions should focus on disseminating the success stories of victims and highlighting practical steps that can be taken to protect and report.
- Cooperation with civil society organizations: Strengthen cooperation with NGOs, associations, and community institutions concerned with protecting children and combating crimes of sexual blackmail and electronic harassment. Workshops, seminars, and awareness programs could be organized in collaboration with these organizations to provide more information, promote awareness, and guide the public on available assistance and support actions.[64]

---

[62] Diaa El-Din Mohamed Radwan, Joint cooperation between the police and the public and its impact on security performance (a comparative study) Factors and means of prevention, PhD thesis, Faculty of Graduate Studies, Police Academy, Cairo, 2018, p. 209.

[63] Mahmoud Ragheb, "The National Council for Women" reveals the punishment for the crime of extortion and how the victim obtains her right, the report of the Egyptian Al-Youm Al-Sabea Foundation, dated April 15, 2023 and available at: https://www.youm7.com/story/2023/4/15/%D8%A7.

[64] Alaa Barrania, "Digital Risk Report: How to Protect Children in the Digital Divide between Generations", Egyptian Center for Strategic Studies and Thought, Cairo, October 15, 2020 and available at: https://ecss.com.eg/11708/.

- Strong legislation and policies: Effective and rigorous legislation and policies must be put in place to combat crimes of sexual blackmail, online child harassment and child sexual exploitation and must include deterrent penalties for perpetrators and swift and effective mechanisms to provide justice to victims.
- Promoting safe technology: Safe technology should be promoted and effective mechanisms developed to monitor and track crimes related to sexual blackmail and online harassment of children. Tech companies should be encouraged to develop tools and techniques to detect, prevent and report these crimes.

12 Conclusion and Summary

12.1 Artificial Intelligence in Combating Online Child Exploitation: A Law-Enforcement Blueprint

The application of artificial intelligence (AI) to the fight against child sexual exploitation (CSE) and child trafficking across the internet, including the dark web, has emerged as both a necessity and a challenge for law-enforcement agencies worldwide. The core mission is to detect, triage, and prioritize suspected child sexual abuse material (CSAM) in order to accelerate victim identification and disrupt criminal activity, while at the same time limiting analysts' exposure to harmful content and ensuring full compliance with legal frameworks. Effective systems must operate in close interoperability with international databases and initiatives such as INTERPOL's International Child Sexual Exploitation (ICSE) database, the U.S. National Center for Missing and Exploited Children's (NCMEC) CyberTipline, and INHOPE's global hotline network.[65]

The operational pipeline begins with lawful data collection. Specialized crawlers, configured to work within anonymity networks such as Tor or I2P, enable investigators to capture text, images, videos, and metadata from illicit forums and marketplaces. These processes are strictly governed by warrants, approvals, and rules of engagement, ensuring that only the minimum required data is collected and that the integrity of the chain of custody is preserved through hashing, logging, and access controls. Once acquired, known material can be screened through perceptual hashing technologies—such as Microsoft's PhotoDNA or PDQ hashing—allowing rapid identification of previously catalogued CSAM and significantly reducing analyst exposure.

Beyond known material, advanced machine-learning techniques are required to detect new and previously unseen content. Computer vision models such as convolutional neural networks (CNNs) and vision transformers (ViTs) can process

[65] European Union Agency for Law Enforcement Cooperation (Europol). Internet Organised Crime Threat Assessment (IOCTA) 2023. The Hague: Europol, 2023. https://www.europol.europa.eu.

images and videos by frame sampling and clip-level scoring. Multimodal systems link textual metadata with images, while natural language processing (NLP) techniques scan posts and private messages for indicators of grooming, enticement, or financial sextortion. Outputs from these models are combined into risk scores that prioritize investigative leads for human review.[66]

AI methods are also being deployed in the analysis of offender networks and financial flows. Graph-based learning uncovers relationships between users, re-used nicknames, and cryptographic keys, helping to surface facilitators and organized groups. Simultaneously, blockchain heuristics trace cryptocurrency transactions to identify laundering schemes, cash-out services, and clusters of addresses connected to illicit activity. These approaches align with Europol's Internet Organised Crime Threat Assessment (IOCTA), which highlights the central role of cryptocurrency in enabling online exploitation.

A critical endpoint of this pipeline is victim identification and takedown. When suspected CSAM is confirmed, cases are routed to ICSE for cross-case matching or to NCMEC for jurisdictional notification. Automated systems such as Canada's Project Arachnid provide a model for large-scale detection and removal notices, enabling rapid disruption of harmful content at global scale.[67]

Core AI components in this domain include perceptual hashing for initial screening, vision classifiers for imagery, temporal models for video, transformer-based NLP classifiers for text, anomaly detection to flag novel patterns, and graph learning to expose hidden facilitators. These tools are integrated into prioritization frameworks that rank investigative leads according to probability of harm.[68]

Safeguards and ethical governance remain central. All operations must be grounded in legal authority, with strict scope controls and auditing. Analyst safety is prioritized by using hash-based triage and redacted interfaces, minimizing direct exposure to CSAM. Privacy principles are applied through data minimization, role-based access, and the use of privacy-preserving technologies such as differential privacy and trusted execution environments. Importantly, human expertise is kept "in the loop" to validate outputs, review potential biases, and authorize referrals for takedown or prosecution.

Despite these advances, significant operational challenges persist. The overwhelming volume of reports—exceeding 36 million CyberTipline submissions in 2023—creates immense strain on investigative resources. The rise of AI-generated CSAM further complicates detection, requiring models to distinguish synthetic content from authentic imagery while maintaining a focus on victim identification.

---

[66] INTERPOL. International Child Sexual Exploitation Database (ICSE): Annual Report 2023. Lyon: INTERPOL, 2023. https://www.interpol.int.

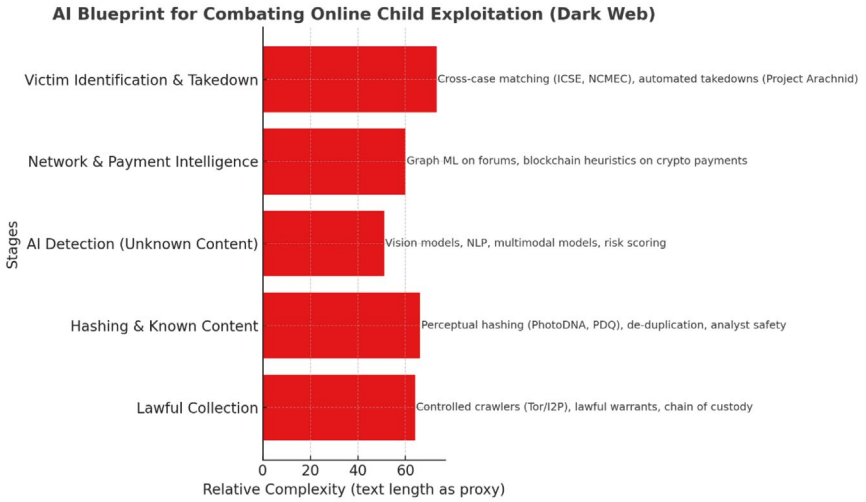
[67] Microsoft. "PhotoDNA: Protecting Children and Detecting Illegal Imagery." Microsoft Research, 2023. https://www.microsoft.com.

[68] Thorn. Child Sexual Abuse Material Detection Using Machine Learning. Los Angeles: Thorn, 2022. https://www.thorn.org.

Adversarial tactics such as steganography, coded language, and invite-only forums continue to evolve, while jurisdictional fragmentation demands constant cross-border cooperation through Europol, INTERPOL, and allied organizations.[69]

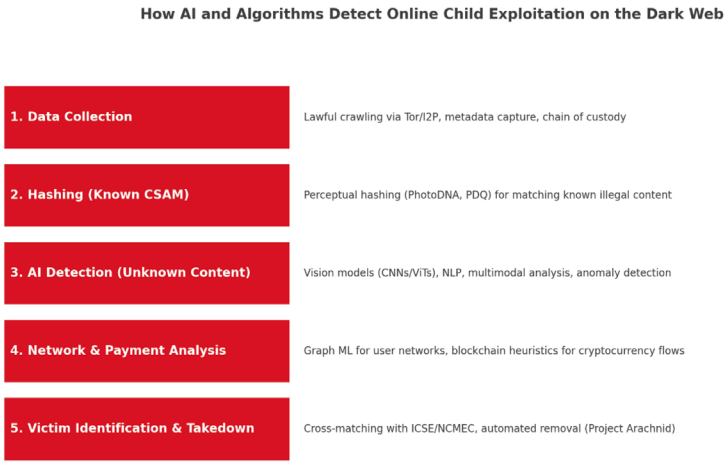
To measure effectiveness, agencies must track key performance indicators (KPIs), including hash-match accuracy and latency, model precision and recall, prioritization gains, victim identification speed, takedown effectiveness, analyst exposure reduction, and overall throughput. These metrics provide accountability and guide iterative improvements.

Finally, AI initiatives should align with established programs and standards. INTERPOL's ICSE forms the backbone for victim identification, while the NCMEC CyberTipline serves as a central reporting hub. Project Arachnid demonstrates automated takedown at scale, and the Technology Coalition provides voluntary principles to guide responsible detection practices. Combined, these frameworks offer a roadmap for integrating AI tools into a coherent, ethically grounded, and globally coordinated response to child trafficking and exploitation online.



I've created both a table and a chart that summarize the AI blueprint stages for combating online child exploitation on the dark web. The table lists each stage with its description, and the chart visualizes their relative complexity.

[69] UN Office on Drugs and Crime (UNODC). Global Report on Online Child Sexual Exploitation and Abuse. Vienna: UNODC, 2024. https://www.unodc.org.



Here's a step-style chart showing how AI and algorithms detect online child exploitation on the dark web—from lawful data collection, through hashing and AI detection, to network analysis and final victim identification/takedown.

The Role of Artificial Intelligence in Committing Child Sexual Abuse on the Darknet: Challenges and Opportunities



Hesham Badawy

1 Introduction

The criminal legislator gave the child [5] special protection, embodying what was stated in successive constitutions, especially the constitution of 2014, as part of the Egyptian state's commitment to international agreements in this regard [17]. The 1989 United Nations Convention on the Rights of the Child **Article 80** of the Constitution enshrines the international standards in force in the field of child protection. The State is obligated to care for and protect the child from all forms of violence, abuse and abuse. It is also committed to establishing a special judicial system for child victims. In application of the advanced standards, the Egyptian legislator has adopted a criminal policy based on tightening penalties if the crime is committed on a child.

This is what is stated in the text of **Article 116 of the Law Child No. 12 of 1996 added by Law No. 126 of 2008**, according to which as an example: The minimum penalty prescribed for any crime in which the victim is a child if it is committed by an adult (or the perpetrator). However, the application of the text of the said article raised some practical problems. Before criminal courts, especially in the field of combining the provision of this article with the punitive provisions in The Penal Code and **Law No. 64 of 2010** on combating human trafficking aggravate punishment, Ii the victim is "i.e., the target of the attack has already thrown" a child. These problems have led to a difference in the penalties level imposed on adults from Identical or at least similar facts—when the victim is a child, in violation of the concept of Perpetrators who occupy symmetric focus should have consistency.

The concept of "consistency" means and that similar cases, like offenders must be treated alike are treated in a similar way. This is done by the nature of like cases are

H. Badawy (✉)
IEEE EGYPT Section, Alexandria, Egypt
e-mail: heshamelbadawy@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_6

treated alike must be treated in a symmetrical manner. The situation is that the sponsors of the principle of "individualization of punishment," which requires a balance between the principles of "consistency" and the "individualization of punishment," and the last principle we will discuss later in more detail.

2 Definitions and Types of Sexual Assault

Sexual assault on children is a heinous crime that causes severe physical, emotional, and psychological harm. It can have long-lasting effects on victims, impacting their lives well into adulthood.

Types of Sexual Assault.

Sexual assault can take many forms, but they all involve an act of sexual violence against another person without their consent. Here are some of the most common types [3, 29]:

A. Rape:

- Penetration rape: This involves the forcible insertion of a body part or object into another person's anus, mouth, or vagina.
- Oral rape: This involves forcing a person to perform oral sex on another person against their will.
- Anal rape: This involves forcing a person to have anal sex against their will.

B. Sexual Abuse:

- Inappropriate touching: This includes touching a person's genitals, breasts, or other intimate areas without their consent.
- Exposure: This involves exposing oneself to another person in a sexual manner without their consent.
- Voyeurism: This involves watching another person undressing or engaging in sexual activity without their knowledge or consent.

C. Sexual Exploitation:

- Child sexual abuse: This involves the sexual abuse of a child by an adult.
- Sexual trafficking: This involves forcing or coercing a person into engaging in sexual activity for profit.
- Sexual assault in institutions: This involves sexual assault that occurs within institutions, such as schools, hospitals, or prisons.

D. Stalking:

- Sexual stalking: This involves following, harassing, or threatening a person with the intent of engaging in sexual activity with them.

E. Digital Sexual Assault:

- Revenge porn: This involves sharing sexually explicit images or videos of a person without their consent.
- Cyberbullying: This involves using technology to harass or threaten a person.
- It is important to note that this is not an exhaustive list of all types of sexual assault. Any unwanted sexual contact or behavior can constitute sexual assault.

F. Orphanage Trafficking.

Orphanage trafficking entails the recruitment and/or switch of a baby right into a residential care facility for a reason of exploitation, such as labor, sexual exploitation and servitude, or baby institutionalization for earnings. Orphanage trafficking has been identified as a shape of baby trafficking worldwide regulation and has been an increasing number of mentioned in many undeveloped countries. Despite the developing instructional awareness in this subject, the specifics of ways kids are targeted, recruited, and transferred into those unregulated orphanages for exploitation stay in large part unclear, as do the ideal social mechanisms employed. Drawing on qualitative research, this text delves into the large function that patron-purchaser relationships play withinside the recruitment, switch, exploitation, and concealment of baby exploitation inside unregulated residential care centers installed for exploitative or earnings reasons in Cambodia and Myanmar. It exhibits how orphanage administrators make the most clientelism to bypass regulations, manage and undermine bureaucratic structures intended to guard inclined groups, and legitimize unlawful sports thru a procedure of formalization.

3 Causes and Factors of Sexual Assault

The causes and factors contributing to sexual assault are complex and multifaceted. While no single factor can fully explain why such acts occur, understanding these contributing elements can help in prevention and response efforts [1, 21, 28].

A. **Perpetrator Factors:**

- **Psychological factors:** Mental health disorders, such as psychopathy or antisocial personality disorder, can increase the risk of perpetrating sexual assault.
- **Cognitive distortions:** Perpetrators may hold distorted beliefs about gender roles, sexuality, or consent, which can justify their actions.
- **Substance abuse:** Alcohol and drug use can impair judgment and increase the likelihood of impulsive behavior, including sexual assault.

- **History of victimization:** Individuals who have been victims of sexual assault or other forms of abuse are at a higher risk of perpetrating such acts themselves.

B. **Victim Factors:**

- **Age:** Children and adolescents are particularly vulnerable to sexual assault due to their physical and emotional immaturity.
- **Disability:** Individuals with disabilities may be at a higher risk of sexual assault due to their dependence on others and limited ability to defend themselves.
- **Social isolation:** Individuals who are socially isolated or lack strong support systems may be more vulnerable to exploitation.
- **Cultural factors:** Certain cultural beliefs or practices may create an environment that allows or condones sexual assault.

C. **Societal Factors:**

- **Gender inequality:** Societal norms and attitudes that reinforce gender stereotypes and power imbalances can contribute to sexual assault.
- **Lack of education and awareness:** Insufficient education about consent, healthy relationships, and the consequences of sexual assault can increase the risk of such acts.
- **Cultural attitudes:** Certain cultural attitudes that normalize or excuse sexual violence can create a permissive environment for perpetrators.
- **Access to resources:** Limited access to mental health services, legal aid, and other support resources for victims of sexual assault can hinder their ability to recover and seek justice.

It is important to note that sexual assault is never the victim's fault. The responsibility for preventing and responding to sexual assault lies with society. By understanding the factors that contribute to this crime, we can develop more effective prevention strategies and support systems for victims.

4 Impact on Victims

- **Physical harm:** Sexual assault can cause physical injuries, including sexually transmitted infections and reproductive health problems.
- **Emotional trauma:** Victims may experience a range of emotional problems, such as depression, anxiety, anger, and difficulty forming healthy relationships.
- **Psychological harm:** Sexual assault can lead to long-term psychological consequences, including post-traumatic stress disorder (PTSD), substance abuse, and eating disorders.

- **Prevention and Support:**

- **Education:** Educating children, parents, and caregivers about sexual assault is crucial for prevention.

- **Open communication:** Creating a safe and supportive environment where children feel comfortable talking about their bodies and experiences.
- **Reporting and investigation:** Encouraging victims to report sexual assault and ensuring that investigations are conducted promptly and thoroughly.
- **Support services:** Providing access to mental health counseling, support groups, and legal assistance for victims of sexual assault.

5 Egyptian Child Law No. 126 of 2008

"Every act or omission thereof (to include the liability of Internet service providers and providers for reporting such Crimes), represented by sending or publishing a pornographic act or represented by preparing, preserving, processing, displaying, printing, publishing or promoting.

Pornographic activities or acts or contact prostitution or pornographic acts…, which was done intentionally by using a system Information, the information network, or similar electronic means, and what is meant here is most electronic means—to achieve that act that requires punishment or precautionary measure."

Based on the definitions of cybercrime in general and cybercrime permissibility in particular, many concepts were extracted.

Related to the crime of child sexual trafficking via the Internet, including what is stated in the Optional Protocol to the Convention on Rights The child related to the sale of children and their exploitation in prostitution and pornography, who defined this type of crime according to a text Article Two of it, which reads as follows: "Exploiting a child in prostitution means using a child for the purpose of sexual activities."

In exchange for a reward or other form of compensation.

– Photographing any child by any means, engaging in real or simulated sexually explicit activities, or any photography

  For the child's sexual organs to essentially satisfy sexual desire.

  Egyptian Child Law No. 126 of 2008 Chapter Eight Criminal Treatment of the child.

  Chapter Eight of the Egyptian Child Law No. 126 of 2008 outlines the legal framework for dealing with children who have committed crimes. It emphasizes a rehabilitative approach, focusing on the child's best interests and their reintegration into society.

  Article (96).

  A child is considered at risk if he is found in a situation that threatens the integrity of the upbringing that must be provided to him in any of the following cases:

1- If his security, morals, health or life are endangered.

2- If the conditions of his upbringing in the family, school, care institutions or other would Be at risk or are at risk of neglect, abuse, violence, exploitation, or displacement.
3- If the child is unjustifiably deprived of his right, even partially, to custody or to see one of his parents or his or her Right to it.
4- If the obligor abandons him to support him or suffers the loss of his parents or one of them or their abandonment or his guardian about responsibility before him.
5- If the child is deprived of basic education or his educational future is endangered.
6- If he is exposed within the family, school, care institutions or others to incitement to violence or immoral acts, pornography, commercial exploitation, harassment, or exploitation sexual or for the illegal use of alcohol or narcotic substances affecting the mental state.
7- If he finds a beggar, it is considered an act of begging to display trivial goods or services or to perform acrobatics and other things that are not suitable as a serious source of subsistence.
8- If he practices collecting cigarette butts or other waste and trash.
9- If he does not have a stable place of residence or usually sleeps on the streets or in other places not prepared for accommodation or overnight stay.
10- If he has contact with delinquents, suspects or those who are notorious for their bad conduct.
11- If he is misbehaving and renegade from the authority of his father, guardian, guardian, or guardian, or from the authority of his mother In the event of death, absence or incapacity of his guardian.
12- If the child has no lawful means of subsistence and no trusted breadwinner In this case, no action may be taken before the child, even if it is an evidentiary procedure, except on the basis of a complaint. From his father, guardian, guardian, mother, or guardian.
13- If the child has no legitimate means of subsistence and no trusted breadwinner.
14- If he suffers from a physical, mental or psychological illness or mental weakness in a way that affects his ability to Awareness or choice so that he fears this disease or weakness for his safety or the safety of others.
15- If the child is under the age of seven and an incident constituting a felony or misdemeanor has been issued. Except in the cases provided for in paragraphs (3) and (4), anyone who presents a child to one of the cases shall be punished. The danger is imprisonment for a period of not less than six months and a fine of not less than two thousand pounds and not exceeding five thousand pounds or with one of these two penalties.

In view of the seriousness of the crimes committed against children, the criminal legislator stipulates in Article 116 bis of Law No. 12 of 1996, as amended by Law No. 126 of 2008 on the child, the need to increase the minimum penalty by the same amount as for any crime in which the victim is a child if it is committed by an adult or if the perpetrator is one of the persons specified in this article, but the application of Article 116 bis of the Child Code has raised some problems before the courts

of first instance and the Court of Cassation. On the types of offences to which the provision of this article may apply, especially if the original punitive provision is subject to aggravating circumstances. Therefore, it has become necessary to address these problems from the rulings issued in this regard, and to clarify the role of the Court of Cassation in ensuring the proper application of this article.

Article (98).

If the child is found in one of the situations of exposure to danger stipulated in items (1) and (2) and items (5) To (14) of Article 96 of this Law, submit his order to the Subcommittee for the Protection of Children for the work of Its affairs provided for in Article 99 bis of this Law, and the Committee may, if it deems it necessary, request. The child's prosecution shall warn the child's guardian in writing to avoid the causes of his exposure to danger. This warning may be objected to before the Children's Court within ten days from the date of its receipt. Such objection and its adjudication shall be the procedures prescribed for objection to criminal orders, and the judgment thereon shall be final. If the child is found in one of the cases of exposure to the danger referred to in the preceding paragraph, after the issuance of the warning Definitively, he submitted his order to the Sub-Commission on Child Protection, to the Committee, as well as to its powers in the preceding paragraph, the child's matter was submitted to the Child Prosecution to take one of the measures stipulated in the Article 101 of this Law, if a child has not attained the age of seven, only a measure shall be taken in respect of him. Delivery or placement in a specialized hospital.

Article (116).

Without prejudice to the provisions of the criminal contribution, any adult who incites a child to commit a misdemeanor or prepares shall be punished. Therefore, he helped him or facilitated it for him in any way and did not reach his intention of that provided that it does not exceed half of the maximum limit for the penalty prescribed for that crime. The penalty shall be imprisonment for a period of not less than six months if the offender uses coercive or threatening means with the child or was one of his ascendants or responsible for his upbringing or observation or was delivered to him under the law or was a servant at any of the above-mentioned persons. In all cases, if the crime is committed against more than one child, even at different times, the penalty shall be imprisonment. A period of not less than one year and not more than seven years. Any adult who incites a child to commit a felony shall be punished by the penalty prescribed for attempting to commit the crime instigate. Or prepare him for that or help him to do so or facilitate it for him in any way and he has not reached his intention in doing so.

Article 116 bis.

The minimum penalty prescribed for any crime shall be increased by the same amount if committed by an adult against a child, or if it is committed by one of his parents or whoever has guardianship or guardianship over him or who is responsible for his observation and upbringing or who has authority over him, or he was a servant of those mentioned above.

116 bis (a) shall be punished by imprisonment for a period of not less than two years and a fine of not less than ten thousand pounds and not exceeding fifty thousand pounds. Anyone who imports, exports, produces, prepares, displays, prints, promotes, possesses, or broadcasts any pornographic works in which he participates, children or related to the sexual exploitation of the child and shall be sentenced to confiscation of tools and machinery used in the commission of the crime and the money obtained from it, and the closure of the places where it was committed, for a period of not less than six months, all with not to prejudice the rights of bona fide third parties. Without prejudice to any more severe penalty provided for in another law, the following shall be punished by the same penalty:

a. Use a computer, the Internet, information networks, or animations to prepare, memorize or to process, display, print, publish, or promote child pornography or exploiting them in prostitution and pornography, defaming or selling them.
b. Use computers, the Internet, information networks, or animations to incite children to delinquency or to be used to commit a crime or to carry out illegal or incompatible activities or acts for etiquette, even if the crime did not actually occur.

Justification and conditions for the application of Article 116 bis achieve the greatest degree of protection for the child in accordance with the international standards in force. The United Nations has paid great attention to the rights of the child in recent decades, culminating in the issuance of the United Nations Convention on the Rights of the Child, 25 years after the adoption of the Convention. (As more countries accede to it, the world becomes more aware of children's rights.) However, despite the existence of an integrated package of international documents in force, countries have been involved in the efforts of preventing and combating human trafficking, children worldwide continue to be exposed to the worst forms exploitation and trafficking, and in many cases, they are treated as a commodity sold and bought from before traders, and international standards are not respected in their treatment if they are trafficked, which may expose them for more abuse (5). Therefore, international documents and organizations working in the field of children's rights national authorities provide the highest standards of criminal protection for children. Among the international standards applicable in relation to the protection of the child "that the child, due to his physical and mental immaturity, needs to special prevention and care, including appropriate legal protection, before and after birth," with. • Dedicating the best interest of the child) 7 The principle of the best interests of the child is the most important one of the legal rules in force in 1) of the Convention on the Rights of the Child and the Protocol) States relating to the rights of the child. Article 3 obliges Optional on the prohibition of the sale of children States with the best interests of the child in mind. The first is through all opinions, as well as the development and implementation of all its visions and policies in light of the best interests of the child. This principle is most clearly reflected in the need to give priority to in the best interest of the child during criminal proceedings. The Optional Protocol on the sale of 3 needs to pay special and primary attention to the principle of interest keepers (children) in its Article 8 Best for the child when national penal systems deal with

child victims of trafficking. Of the Child Law the Egyptian legislator has enshrined the principle of the best interest of the child in national legislation, Article III, last paragraph, of the Child Act stipulates that "the protection of the child shall be And his best interests are the priority in all the cases during the procedures related to childhood, regardless of the party which it issues or initiates." Thus, the principle of the best interest of the child requires that the child is above all consideration, priority and priority in all circumstances, whatever the interests of the parties other. The importance of the principle is evident during interviews and discussions with the child victim during Stages of evidence gathering, investigation and during trial proceedings Article 2 of Law No. 64 of 2010 on combating human trafficking states: Anyone who deals in any way with a natural person, including selling, commits the crime of human trafficking. or offer for sale, purchase or promise thereof, use, transport, delivery, accommodation or reception or extradition whether within the country or across its national borders—if this is done by the use of force or threat of violence, or by means of abduction, fraud, deception, or abuse of power, or taking advantage of the situation of weakness or need, or promising to give or receive sums of money or clothing in exchange for obtaining The consent of a person to traffic in another person over whom he has control—and all this—if the transaction is intentional exploitation in any form, including exploitation in prostitution and other forms of exploitation sexual, exploit.

We can notice the following key provisions for the enforcement for this law:

1. Special Procedures:

- Juvenile Courts: Children who commit crimes are tried in specialized juvenile courts.
- Confidentiality: Proceedings are held in private to protect the child's identity and privacy.
- Legal Representation: Children have the right to legal representation.

2. Rehabilitation and Social Integration:

- Rehabilitation Programs: The law prioritizes rehabilitation programs designed to address the underlying causes of the child's behavior and to reintegrate them into society.
- Educational and Vocational Training: Children may be enrolled in educational or vocational training programs to equip them with skills for future employment.
- Psychological Counseling: Psychological counseling is provided to help children overcome any emotional or behavioral issues.

3. Detention as a Last Resort:

- Detention Centers: Detention centers for children are designed to be rehabilitative and should only be used as a last resort.

- Strict Conditions: Detention conditions must adhere to international standards for the treatment of children in detention.
- Limited Duration: Detention periods are limited and subject to regular review.

4. Protection from Exploitation:

- Prevention of Exploitation: The law prohibits the exploitation of children, including their involvement in criminal activities.
- Protection Measures: Measures are taken to protect children from being influenced or exploited by adults.

5. International Cooperation:

- Cross-Border Issues: The law addresses issues related to cross-border child offenses, including extradition and mutual legal assistance.

Overall, Chapter Eight of the Egyptian Child Law aims to balance the need for justice with the protection of children's rights. It emphasizes rehabilitation and reintegration, rather than punitive measures, and seeks to provide children with the opportunity to become productive members of society.

6 Taskforces of the Anti-Human Trafficking Unit of the Egyptian National Council for Motherhood and Childhood

First: Executive Track:

1. Preparation and enforcement of a national plan.

It was included in the national plan to combat human trafficking announced by the National Committee to Combat Human Trafficking in December 2010 and followed up on its implementation in coordination with the active partners, namely the National Committee, the Ministries of Foreign Affairs, Social Affairs, Interior Justice, the Public Prosecution, civil society, and the International Organization for Migration.

2. Approving a national referral mechanism "National referral mechanism to support victims of human trafficking approved by the National Committee to Combat Human Trafficking" and established in accordance with Law 64/2010.
3. Capacity building and specialized mechanisms The Anti-Human Trafficking Unit continues the efforts it has started since 2008 about awareness-raising for those in charge of the criminal justice administration (Ministries of the Interior, Justice and Public Prosecution), community actors (clerics, teachers, media professionals) and those dealing with victims (civil society organizations and health

workers). These training courses came within the framework of the implementation of national legislation and international conventions to combat trafficking in human beings, which uphold the rights of the victim, and national legislation imposes strict penalties on the offender commensurate with the gravity of the crime, and these courses also come within the framework of the implementation of the above-mentioned national action plan, which is based on four principles: prevention, protection, prosecution, and participation.

- Those in charge of administering justice (Ministries of Interior and Justice and Public Prosecution) to effectively implement the law.
- Actors in society (clerics and media professionals) to inform them of their role in raising awareness of the paths of this crime.
- Those dealing with victims directly from civil society organizations and health workers, in which the focus was on ways to identify victims and provide them with social and health services.
- Training courses for diplomats in the Department of the Diplomatic Corps to emphasize their pivotal role in protecting Egyptian citizens abroad who may be victims of such a crime.

4. Protection, recovery, and reintegration of victims: The unit encouraged civil society organizations to network by training more than 100 specialists from 48 NGOs at the level of 5 governorates in the field of recovery and rehabilitation of victims, which resulted in the formation of a national coalition of NGOs to combat human trafficking headed by the Center for Egyptian Women's Issues, and to support rehabilitation and reintegration services, several homes were established to provide protection and rehabilitation services for victims psychologically, socially and healthily, and the rehabilitation of children in cooperation with the Belgian VIS, the International Organization for Migration and the Catholic Relief and Freedom Society.
5. Databases The unit succeeded in developing a database classified according to age, sex, geographical location, and socio-economic background, and the prosecution provided data related to victims, whether related to human trafficking cases in which the perpetrators were punished, or considered before the Public Prosecution within the framework of crimes classified in accordance with international conventions and national legislation, and studies were conducted in the governorates of (Giza, Assiut, Aswan, Luxor, and Qena), and a study is being implemented in Fayoum Governorate, which includes a qualitative and quantitative analysis on the root causes behind the spread of all crimes referred to. Previously.
6. Efforts to prevent forced labor ("Decent Work for Domestic Workers, Especially Children and Women" initiative), where a national working group was formed that includes in its membership the National Coordinating Committee to Combat Human Trafficking, the Ministry of Manpower, the International Organization for Migration, the United Nations Women, the Shehab Foundation, the Egyptian

Women's Legal Assistance Foundation, and the National Coalition to Combat Human Trafficking.

7. The axis of raising awareness and activating reporting mechanisms with the aim of raising awareness of the harm of the basic arguments used by employers to justify their exploitative and aggressive behavior against maids, strengthening the role of the media and civil society in mobilizing society to support this issue, implementing awareness campaigns, and practical plans to improve employers' behavior away from legislative variables, in order to change many misconceptions and preconceived ideas about domestic workers, and the acceptable type of employer behavior, and educating the maids themselves about reporting mechanisms and the concerned authorities.
8. The focus of prosecution, by imposing penalties on abusive employers and forcing them to pay fines and announcing these penalties in order to convey the message that such behavior is unacceptable.

Second: Promotional and Legislative Tracks:

1. Publication of legislation and literature: Printing national legislation and issuing guidelines for law enforcement officials to combat trafficking in human beings and ways to identify victims in cooperation with the International Organization for Migration It was circulated to the Ministries of Justice, Public Prosecution and Interior, the Ministry of Social Affairs, the Centre for Social and Criminal Research, the Ministry of Education and the governorates, and crimes that may come into contact with it, such as the crime of smuggling migrants. The guide focuses on human rights principles, stressing that measures to combat trafficking in human beings should not adversely affect human rights and the dignity of persons, in particular the rights of victims of trafficking in human beings. The guide provides a full chapter on how to provide protection to victims and witnesses, how to identify, deal with them, and assess the risks that surround them. It also explains ways to train teachers to educate students about crime patterns, and another guide for social workers in charge of care homes for victims.
2. Prosecution and Law Enforcement: Cooperation with the Public Prosecution to prosecute and punish perpetrators, which contributed to changing policies related to the arrest and prosecution of perpetrators in implementation of the law, and supporting children to return to school, and a guide is being issued from the Public Prosecution regarding what legal and administrative rights victims must be informed of as they are exempt from legal accountability, and the importance of voluntary progress to assist the authorities to combat crime in accordance with Chap. V, in particular Articles 22, 23, and 24, and permanent points of contact are being identified that will facilitate victims' access to Egyptians and non-Egyptians on their rights, in coordination with the Public Prosecution within a legal framework.
3. Regional cooperation with the League of Arab States: in the implementation of the Arab plan to combat human trafficking, especially the legal department "Coordination Unit to Combat Human Trafficking," where the unit trains the League's work team.

4. Definition of human trafficking: Human trafficking is defined as "children and women" in accordance with Law 64 of 2010, the Palermo Protocol, the amended Child Law, penalties, civil status, and Law No. 5 regulating organ transplantation, provided that dealing with human beings for the purpose of exploitation, through kidnapping, fraud, deception, abuse of power, or exploitation of the state of weakness or need by placing him under control, limiting his movement, forcing him to forced labor, or carrying out illegal acts in exchange for profit, and obtaining a financial benefit or reward, from Before an individual, or gang organized internally or transnationally. The Egyptian legislator has expanded the definition of human trafficking to include many types of exploitation that change and follow rapidly because the nature of the crime of human trafficking is unique, as it is a multifaceted crime whose parties are intertwined and multiple, and exacerbated in light of natural disasters and wars, political, security, and economic changes, and the accompanying poverty and unemployment, and security liquidity that increases crime rates, not to mention the tremendous development in information and communication technology.

7 Definition of the Sale of Children

The definition of all cases of sale and prohibition of children in accordance with Article 291 of the Penal Code, Article 116 bis (a) of the Child Code, and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography, although similar to the concept of trafficking in human beings, is not the same, as trafficking involves recruiting a child by traffickers, transporting, harboring, or receiving him for the purpose of exploitation. The child is sold, or not sold, meaning that the sale is not an essential element of the child trafficking process which requires that the sale of children be accompanied by any act or transaction whereby a child is offered, handed over or accepted, in any way whatsoever, by any person or group of persons to another person in exchange for remuneration or any other form of compensation; sex in exchange for reward, or any other form of compensation; child pornography, by any means, real or simulated sexual activities or any depiction of the sexual organs of a child primarily for sexual gratification, producing, distributing, publishing, importing, exporting, offering, selling, or possessing child pornography; is appropriate to establish the adoption of a child in breach of applicable national legislation on adoption; or any attempt to commit any of the above acts or to collude in or participate in any of them within the country or across borders, even if the crime has not been committed.

8 Child Sexual Abuse Resources in the Digital Era

In the1970s and early1980s, the climate toward adults having sexual relations with minor was more open than it is today, due in part to the sexual revolution, but even then, sexual attraction to underage children was generally considered a typical. In that era, those attracted to minors gathered in support groups, where fantasies were openly discussed among like-minded participants. Usually, to avoid the attention of law enforcement, the organizers of such support groups ensured that **child sexual abuse materials (CSAM)** were not openly exchanged at these meetings. Although illegal, those interested in CSAM could resort to adult book stores that sold specialized magazines or order periodicals containing sexually explicit images of underage children by regular mail. Public opinion and lawenforcementpracticeinthe1990s tended toward a less permissive attitude, in part because of several highly publicized incidents of child sexual abuse. In response, many local support clubs disbanded, and adult bookstores narrowed their selection to avoid prosecution.

The rise of the Internet brought new opportunities. Following the success of Napster, a peer-to-peer network that allowed users to search for music files on local disks on neighboring computers and download them directly when found, a broader peer-to-peer network developed, facilitating the sharing of digital images and movie clips sharing of digital images and movie clips also became easier. Images and films that were found and shared included CSAM. The rise of social media also created dedicated online forums focused on "child love". Previously, support groups were a regional affair, and their clients were mostly people in the city where they were held. Social media has changed this, allowing interaction with like-minded people from around the world. However, as with offline support groups, the moderators of these forums had to be careful that members did not commit crimes in the forum environment. Although visitors to these forums communicated online using nicknames, they were keenly aware that their true identities could easily be revealed by hackers and police.

Darknet alleviated their fears of their true identities being revealed. By hosting a forum web site accessible only to other TOR users, Darknet provided an ideal platform for creating an online space where people with a sexual interest in minors could gather and freely discuss their thoughts and feelings without fear of being identified. The Darknet provided the ideal platform. The anonymity offered by the Darknet also provided a new venue for accessing and exchanging CSAMs, bringing together supply and demand on an unprecedented global scale. The prolife ration of smart phones equipped with sophisticated cameras also blurred the distinction between consumer and producer, further increasing the volume of CSAM in circulation. Today, Darknet CSAM forums are the center of a global online community of hundreds of thousands of individuals with a sexual interest in children.

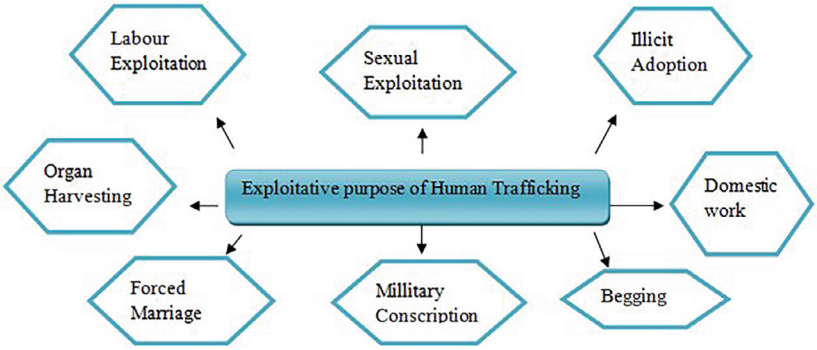


Fig. 1 Flow chart of some exploitative purpose of human trafficking [37]

9 AI Is Revolutionizing the Fight against Human Trafficking

Some of the ways AI and companies like ***"Veritone"*** are helping law enforcement and government agencies combat human trafficking is by enhancing human capabilities and efforts to create faster, more streamlined, and more accurate processes. This includes advanced data analysis, pattern identification, and proactive intervention Fig. 1.

10 AI-Enhanced Data Analysis

AI-powered data analysis will revolutionize the fight against human trafficking. By analyzing large data sets, hidden patterns can be discovered, and complex trafficking network scan be revealed. The technology will also enhance communication and collaboration between LEAs and government organizations, enabling faster and more efficient responses.

Tools such as Veritone Track further assist investigators by streamlining the process of tracking individuals and locating critical information without the use of personally identifiable information (PII). This is especially helpful in tracking people of interest or missing persons across various camera footage.

11 Veritone AI Software

Veritone's operating system for artificial intelligence, aiWARE™, orchestrates a diverse ecosystem of machine learning models to transform audio, video, text, and other unstructured data sources into actionable intelligence. In addition, multifaceted

aiWARE™ platform capable of listening, watching, analyzing, and optimizing the world's information and infrastructure 24/7/365. The cognition behind aiWARE™ is being used extensively across major commercial enterprises and Government & Regulated Industries customers today, driving down the cost, complexity and time to develop, deploy and distribute cognitively enabled applications across any cloud or on-premises infrastructure. On the other hand, industry leading partners and customers include a great group of companies such as: Amazon, Microsoft, and CNN. Veritone's proven Enterprise AI platform, aiWARE™, is the foundation upon which Veritone is concerning in helping customers and partners: to build AI-powered solutions and applications faster and cost effectively. Also, Veritone is accelerating AI enterprise implementation and adoption, increasing operational efficiency. This is done to leverage a vast ecosystem of proprietary and third party by means of optimized AI models with minimal integration costs. Figure 2 illustrates the Veritone aiWARE Platform.

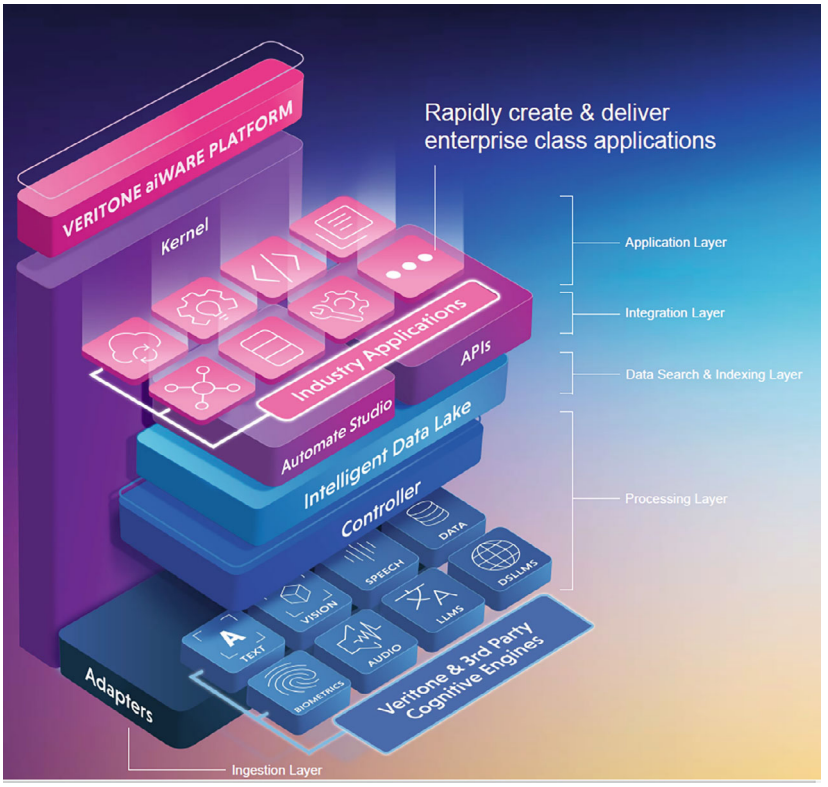


Fig. 2 Veritone aiWARE Platform [39]

12 AI in Victim Identification

By using its capacity to evaluate internet content and identify possible indicators of human trafficking, artificial intelligence (AI) plays a significant role in victim identification. Using algorithms for risk assessment, this technology assists LEA in prioritizing cases.

Public safety organizations can improve their capacity to locate and rescue victims by utilizing AI, which will guarantee a route to victim recovery and trafficker conviction. The identification process is aided by tools like Veritone IDentify, which compares an image of a victim with their face across law enforcement databases, including arrest record scans. Veritone Track's human like object (HLO) detection is a practical and very successful substitute for facial recognition technology for businesses.

13 AI in Suspect Identification

Suspects have been identified and captured with the help of artificial intelligence (AI) that can examine social media and other internet platforms to examine suspicious behavior. AI can also help with cross-border investigations by making it easier for LEAs to share information.

Veritone IDentify and Track enhances the effectiveness of suspect identification by integrating easily with current software and processes, facilitating quicker case resolution and trafficker capture.

To determine the seven criteria for trustworthy AI as well as the state of face processing apps and tasks in light of the recently passed European AI laws. Face processing operations must be constructed on top of the seven pillars that make up dependable AI. In the context of particular intended objectives and specific usage scenarios, face processing applications—real-world use cases that make use of one or more face recognition tasks—are covered by the AI law. Fig. 3 illustrates the face processing tasks.

14 Challenges and Ethical Considerations in Combating Human Trafficking Using AI

In order to avoid overreliance on AI and maintain ethical decision-making in combating human trafficking, it is essential to strike a balance between technological advances and human judgment.

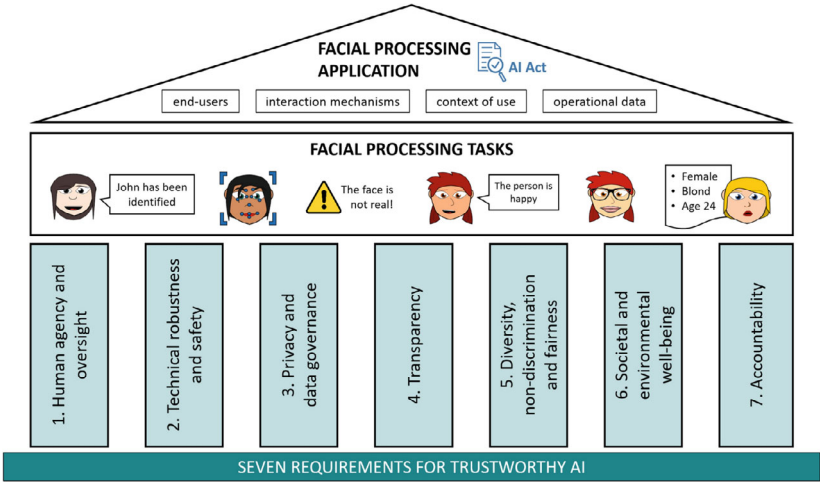


Fig. 3 AI Facial Processing Tasks [2]

AI-based anti-trafficking efforts need to consider three key points: ensuring data privacy and protection through the involvement of sensitive (or confidential) information, addressing bias in AI algorithms to prevent discrimination, and setting a framework for transparency and accountability in AI systems [12, 40].

Important Example of the AI's Role in Combating Human Trafficking May be Dramatic Cases as in Orphanage Trafficking.

Orphanage trafficking is a heinous crime that involves the illegal removal, sale, or trade of children from their families or communities. AI can play a crucial role in combating this issue by providing innovative solutions to detect, prevent, and address this crime.

Here Are Some Ways AI Can Be Utilized:

1. Identifying and Analyzing Patterns:

- **Data Mining:** AI can analyze large datasets of orphanage records, adoption records, and travel documents to identify patterns of suspicious activity.
- **Network Analysis:** AI can map out complex networks of individuals involved in trafficking, including brokers, corrupt officials, and adoptive parents.
- **Predictive Modeling:** By analyzing historical data, AI can predict potential trafficking hotspots and target preventive measures.

2. Detecting and Verifying Child Identities:

- **Biometric Analysis:** AI-powered biometric systems can verify the identities of children, ensuring they are not being trafficked under false pretenses.

- **Facial Recognition:** AI can compare photos of children to identify potential victims and track their movements.

3. Monitoring Online Activities:

- **Social Media Surveillance:** AI can monitor social media platforms for suspicious activity related to child trafficking, such as the sale or adoption of children.
- **Darknet Monitoring:** AI can be used to scan the Darknet for illegal activities related to child trafficking, such as the sale of children or the sharing of child exploitation material.

4. Facilitating International Cooperation:

- **Data Sharing and Analysis:** AI can facilitate the sharing and analysis of data across borders, allowing law enforcement agencies to collaborate more effectively.
- **Real-time Information Exchange:** AI-powered systems can enable real-time information exchange between different countries, helping to track traffickers and rescue victims.

5. Raising Awareness and Education:

- **AI-Powered Educational Tools:** AI can be used to create interactive and engaging educational tools to raise awareness about child trafficking and its consequences.
- **Public Awareness Campaigns:** AI can help analyze data to identify target audiences for public awareness campaigns and tailor messages to specific demographics.

By leveraging AI, we can enhance our ability to detect, prevent, and investigate cases of orphanage trafficking. This technology can be a powerful tool in the fight to protect vulnerable children and bring perpetrators to justice.

Figure 4 illustrates the results as related to the first set of six components. The labels on the second level refer to the components and the labels on the third level refer to the reasons as provided by the participants for the importance of each component. *Yellow* labels refer to the components (1) promoting knowledge on child abuse, *orange* labels to (2) learning about secrets, *light green* labels to (3) increasing awareness of children's rights, *turquoise* labels to (4) learning to avoid self-blame, *dark green* labels to (5) learning about own body and boundaries, and *brown* labels to (6) identifying trusted persons. n = the number of participants, [27].

Figure 4 illustrates the results as related to the second set of six components. The labels on the second level refer to the components and the labels on the third level refer to the reasons as provided by the participants for the importance of each component. Red labels refer to the components (7) increasing social–emotional skills, dark blue labels to (8) recognizing and avoiding risky situations, pink labels to (9) increasing assertiveness skills, light blue labels to (10) learning to go away from a potential abusive situation or to find help, white labels to (11) increasing a child's

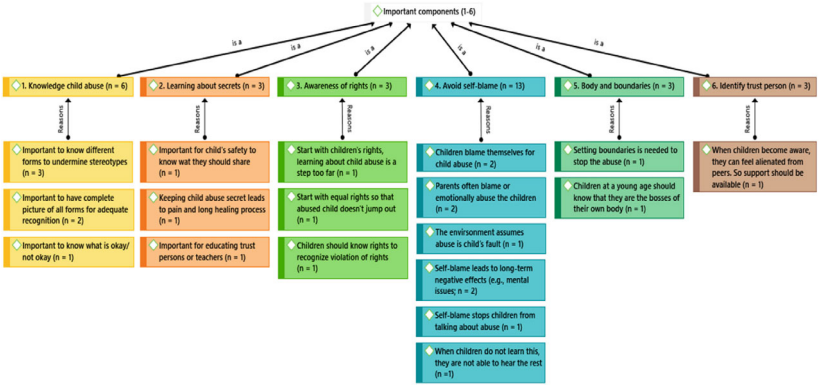


Fig. 4 (**a**). First set of School-Based Programs for Child Abuse Prevention for AI Data Analysis [27]. (**b**). Second set of School-Based Programs for Child Abuse Prevention for AI Data Analysis [27]

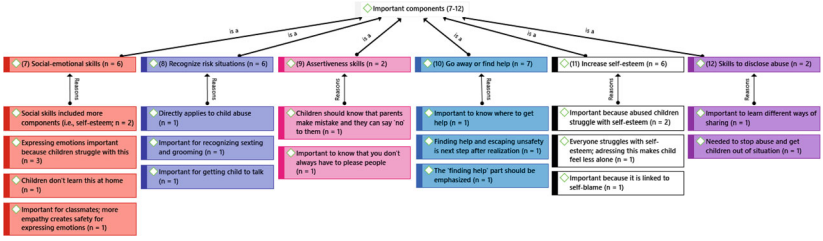


Fig. 4 (continued)

self-esteem, and purple labels to (12) learning skills to disclose abuse. n = the number of participants [27].

15 Privacy and Data Security Concerns

The use of AI for trafficking prevention raises important privacy and data security concerns. While information sharing is essential for effective intervention, it must be balanced with respect for privacy rights.

Protecting sensitive data is critical to safe guarding the identity and confidentiality of victims, witnesses, and informants. Measures should be taken to ensure data security, such as encryption and strict access control.

Furthermore, clear guidelines and regulations are needed to prevent misuse of collected data and to hold responsible parties accountable. Maintaining the right balance between information sharing and privacy is essential to maintaining trust and

effectively combating trafficking. Prejudice and discrimination in AI carefully developed and implemented, AI algorithm scan will lead to unfair targeting and profiling of certain individuals and groups. To address these concerns, transparency in the development and implementation of AI systems is critical. This includes diverse and representative data sets, regular audits, and ongoing assessments to identify and correct biases ethical guidelines should be established to ensure fairness, accountability, and nondiscrimination in AI-based anti-trafficking efforts [6, 7].

16 Legal and Regulatory Framework

International coordination and cooperation among governments, organizations, and stakeholders raises essential to establish a comprehensive framework that transcends national borders. Such a framework should emphasize transparency, accountability, and ethical considerations in AI implementation.

The right framework will help ensure that AI technology is used responsibly and effectively to combat human trafficking, while at the same time protecting the right individuals.

17 Real-World Examples of AI Fighting Human Trafficking

A. **AI-driven Success Stories.**
Another example is the partnership between the NGO. They developed a "spotlight" tool that uses AI to analyze online platforms and identify potential child trafficking victims. This technology helps law enforcement prioritize cases and identify victims faster, leading to more effective interventions and improved outcomes for victims. Figure 5 illustrates the flow chart of human trafficking.

B. **AI in the Fight Against Human Trafficking.**
Artificial Intelligence (AI) is emerging as a powerful tool in the global fight against human trafficking. By analyzing vast amounts of data and identifying patterns, AI can help detect and disrupt trafficking networks, identify victims, and bring perpetrators to justice.

Here are some key examples of how AI is being used to combat human trafficking:

1. Identifying and Analyzing Online Trafficking Ads:

- Keyword and Image Recognition: AI algorithms can scan online platforms like social media and Darknet marketplaces to identify keywords and images associated with human trafficking.

- **Pattern Recognition:** AI can identify patterns in online advertisements, such as repetitive language, specific phrases, or coded language, that may indicate trafficking activities.

2. Detecting and Analyzing Social Media Activity:

- **Social Media Monitoring:** AI tools can monitor social media platforms for signs of exploitation, such as unusual activity, suspicious language, or changes in behavior.
- **Network Analysis:** AI can analyze social networks to identify potential victims and traffickers, as well as uncover hidden networks.

3. Analyzing Financial Transactions:

- **Identifying Unusual Financial Activity:** AI can analyze financial transactions to detect unusual patterns that may be associated with human trafficking, such as large sums of money moving through specific accounts or suspicious wire transfers.

4. Developing Digital Forensics Tools:

- **Data Extraction and Analysis:** AI-powered tools can help extract and analyze digital evidence, such as phone records, emails, and social media messages, to identify victims and perpetrators.

5. Creating AI-Powered Chatbots:

- **Victim Support and Outreach:** AI-powered chatbots can provide support and information to victims of human trafficking, offering a confidential and accessible way to seek help.

6. **Organizations and Initiatives Leveraging AI:**

- **Thorn:** This organization uses AI to identify and remove child sexual abuse material from the internet.
- **Polaris Project:** This organization uses AI to analyze hotline data and identify trafficking patterns.
- **Global Emancipation Network (GEN):** GEN uses AI to analyze online advertisements and identify potential victims of sex trafficking.

By harnessing the power of AI, law enforcement agencies, NGOs, and technology companies can work together to combat human trafficking more effectively, protect victims, and bring perpetrators to justice.

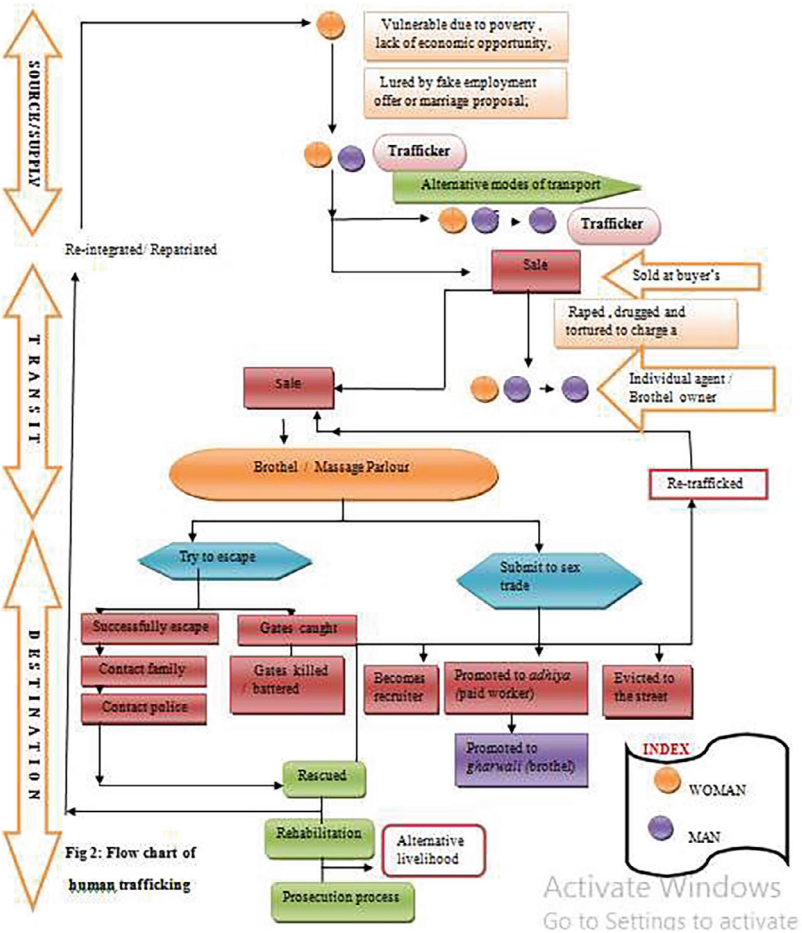


Fig. 5 Flow chart of human trafficking [10]

C. **Partnerships and Collaboration.**

NGOs and organizations are at the fore front of promoting the adoption of AI in the fight against human trafficking. For example, the Polaris Project is using AI to analyze hotline data and identify patterns of trafficking. This technology is enhancing response capabilities and identifying emerging trends in real time, improving victim assistance and enabling strategic interventions.

In addition, collaboration between Academia and law enforcement has also led to significant advances. Researchers at Carnegie Mellon University have developed an AI-based tool called **TraffickJam** that compares images uploaded by hotel guests with a database of known trafficking locations. This innovative approach has helped law enforcement agencies identify, locate, and arrest trafficking suspects and networks [32].

These examples illustrate the power of AI and the potential impact of partnerships and collaborations. By harnessing AI's capabilities, leveraging its expertise, and facilitating cooperation, public safety agencies can make significant strides in combating these incidents.

D. **The Future of AI in the Fight Against Human Trafficking.**
New technologies and innovative solutions such as natural language processing (NLP) can analyze text and voice to detect indicators of trafficking in online communications, helping to identify both victims and traffickers, leading to more proactive intervention. In addition, advances in computer vision will enhance the analysis of images and video to detect visual cues and patterns associated with trafficking.

18 AI-Generated Child Sexual Abuse Material (AIG-CSAM)

Nevertheless, it is imperative that the future of Generative Artificial Intelligence (GAI) in combating trafficking be approached with prudent and ethical considerations. GAI may use of Visual depiction (image/video) of sexually explicit conduct involving a minor, the creation of which has been facilitated by generative AI technologies. This may range from a fully generated image/video, to generated elements applied to a pre-existing image/video. Safeguards must be in place to address potential biases, ensure privacy protection, and mitigate unintended consequences. Transparency, accountability, and ongoing evaluation of GAI systems are essential to maintain trust and protect human rights [23, 38].

We may have to discriminate between two main categories related to GAI in child abuse, namely: Child sexual abuse material (CSAM), and child sexual exploitation material (CSEM). So, the child sexual abuse material (CSAM) may concern about the visual depiction (image/video) of sexually explicit conduct involving a minor. Does not require that the material depicts a child engaging in sexual activity. Covers lewd and lascivious content, as well as content with a focus on genitalia. On the other hand, Child sexual exploitation material (CSEM), which is used to describe image/video/audio content sexualizing children, grooming text, sexual extortion text, CSAM advertising, CSAM solicitation, and text promoting sexual interest in children.

This section outlines a series of recommended mitigations to implement these principles.

The purpose is to make it more difficult for malicious actors to exploit GAI technology to create AIG-CSAMs and CSEMs.

For each recommended mitigation measure, may have the following.

—The intended impact of the mitigation measure and an estimate of the expected impact of the mitigation measure (one of the following).

"incremental" (a positive step) or "significant" (an intervention that will transform the situation).

—Scope of mitigation measures: "narrow" (can be implemented by one organization alone), "moderate" or "broad" (can be implemented by one organization alone), Moderate" or "Extensive" (may require coordination and collaboration among multiple organizations or stakeholders.)

—Variables that can be expanded or reduced when addressing that mitigation measure.

—Whether related to AI developers, AI providers, data hosting platforms, social platforms, searches engines.

—Close drooping organizations?

—Resources to more easily implement mitigation measures.

Informational "(intended to provide additional background information or as an example of mitigation measures) or" implementation" (intended to highlight possible solutions and solution providers).

The GAI maintain (as an expression) refers to the process of maintaining the quality of ML/AI models in case of data diversion or trending and changing landscape [14]. Figure 6 illustrates the cases of possible mitigation scenarios for protecting children.

Mitigations

SIGNIFICANT IMPACT · OPEN SOURCE · CLOSED SOURCE

MAINTAIN OVERVIEW	AI Developers	AI Providers	Data Hosting Platforms	Social Platforms	Search Engines
1 Remove services for "nudifying" images of children from search results					✓
2 When reporting to NCMEC, use the Generative AI File Annotation	✓	✓	✓	✓	
3 Detect and remove from your platforms known models that were explicitly built to create AIG-CSAM		✓		✓	✓
4 Retroactively assess currently hosted generative models, updating them with mitigations in order to maintain platform access	✓	✓			
5 Detect, report, remove and prevent CSAM, AIG-CSAM and CSEM on your platforms				✓	
6 Invest in tools to protect content from AI-generated manipulation	✓			✓	
7 Maintain the quality of your mitigations	✓	✓	✓	✓	✓
8 Disallow the use of generative AI to deceive others for the purpose of sexually harming children. Explicitly ban AIG-CSAM from your platforms.				✓	
9 Leverage Open Source Intelligence (OSINT) capabilities	✓	✓		✓	

Fig. 6 Possible mitigation scenarios for protecting children

19 Role of AI and Connecting it to the Matter of Darknet

Agencies such as WeProtect [16] Global Alliance and the Internet Watch Foundation (IWF) sounded the alarm regarding AI CSAM in 2023, highlighting it as an area of concern for governments, civil society organizations, private sector agencies, and parents and children. IWF's 2023 research found that offenders are taking images of children, often famous children, and applying deep learning models to create AI CSAM.

There are currently two major categories of AI CSAM: (1) AI-manipulated CSAM, where images and videos of real children are altered into sexually explicit content, and (2) AI-generated CSAM (AIG-CSAM) in which entirely new sexual images of children are manufactured. IWF reported in 2023 that both types of AI CSAM are prevalent.

Data collection was conducted in January 2024 using a key word search in the "Atlas" dataset of Darknet child sexual exploitation (CSE) forums in Voyager. Our search using the search terms "AI" or "Artificial intelligence," and the search date range 2023 (12 months), resulted in 19,951 results (this included 9675 hyperlinks; 9238 posts; 1021 threads; and 17 forum profiles). We then looked at a sample in order to conduct some preliminary analysis of what forum members were saying and doing regarding AI CSAM.

The discovered issues are very worrying. First, there is a real appreciation and appetite for AI CSAM. Darknet Forum members refer to those who are creating AI CSAM as "artists." What forum members appreciate is that those creating AI CSAM can take an image of, for example, a victim child film character, and create a plethora of AI CSAM of that child. At present, forum members are particularly interested in AI CSAM of famous children such as child actors and child sports stars.

The AI era is being used to deliver child sexual abuse material (CSAM), which is a widespread and growing threat, according to the Internet Watch Foundation (IWF). In October 2023, our initial investigation found that more than 20,000 artificial intelligence (AI)-generated images were posted on a Darknet discussion board in a single month, with over 3000 of those images showing crooked infant sexual assault. Since then, the challenge has increased and continues to change.

Figure 7 illustrates steady increase in the number of reports in which an analyst has detected any form of AI-generated material (in red), as well as a subset of these numbers, reports in which AI CSAM has been recognized and "actioned"—processed as a criminal offense under UK law (in gray). The IWF wants "actioned" AI CSAM taken down from the internet.

Notably, we have seen AI CSAM images being shared on commercial sites on the clear web—in place of "real" images of children. These include dedicated commercial banner sites, and forum pages with affiliate file hosting links [8].

In addition, it was discovered that these forum members' who are creating AI CSAM are not IT, AI, or machine learning experts. They are teaching themselves how to create AI CSAM. They easily access online tutorials and manuals on how to create AI CSAM; these resources are widely shared in Darknet forums. They

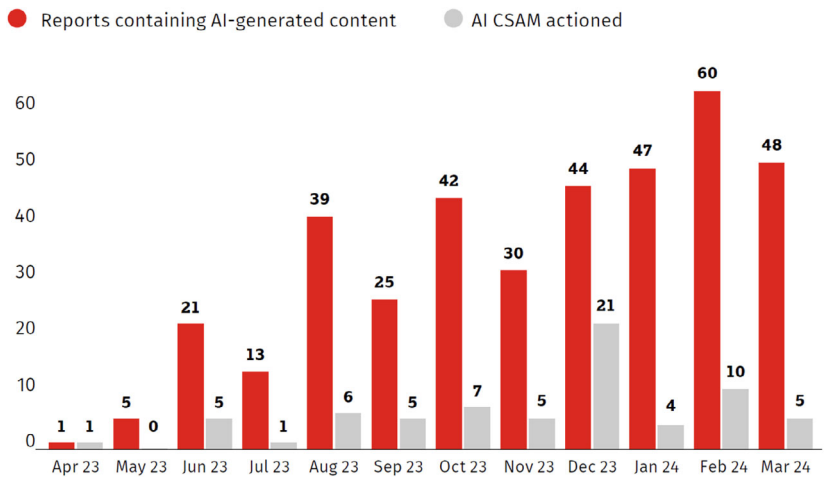


Fig. 7 IWF reports containing AI-generated content, March 2023 to April 2024 [8]

then reach out to other Darknet forum members who already have experience in creating AI CSAM to ask questions about how to 'train' the software and overcome challenges that they are experiencing (such as the child in the image having too many limbs or digits). As part of this effort to improve their AI production skills, forum members actively request others to share CSAM so that they can use this material for 'practice'.

It is discovered that some forum members are already moving from the creation of what they describe as "softcore'" AI CSAM to more "hardcore" material. Driving this pattern may be the normalization and desensitization of material and the search for more explicit and violent material.

It was also clear that CSAM forum members are hopeful that AI will continue to quickly develop so that soon they won't be able to tell if a sexual image of a child is real or not. They're also hopeful that AI will develop to a point that they can create increasingly hardcore and interactive material (such as interactive videos where they can instruct a video character to perform sexual acts).

We must limit the expansion of the phenomenon through legal reform, robust deterrence measures, as well as further evidence generation, and awareness-raising of the issue.

20 Conclusion

The presented work concluded that child sexual abuse material (CSAM) has become so spread on the Internet and Darknet. The evolution of such offensive materials is growing fast. Artificial Intelligence has a main role of generating such abuse

materials (AIG-CSAM). The role of AI and Darknet is notably succeeded due to many factors, such as encrypted online content not indexed by conventional search engines. In addition, the Darknet can only be accessed using specific browsers like TOR Browser.

Organized criminal developers and producers have moved some of their activities to virtual reality, exploiting the Darknet as a black market and a fertile environment for CSAM activities. Estimates indicate that these organized groups have greatly profited from these illicit activities, relying on encrypted virtual currencies.

Darknet has a great role in the increasing of CSAM activities on the web. In addition, AI with Darknet is working side by side to enlarge the distributions of the abuse materials.

Countries and international organizations relevant to combating organized CSAM activities are making strenuous efforts to confront organized criminal activities committed on the Darknet despite the difficulty of tracking them due to encryption techniques.

References

1. American Psychological Association. (2023). Paraphilia. APA Dictionary of Psychology. https://dictionary.apa.org/paraphilia
2. Anda, R.F., Felitti, V.J., Bremner, J.D. et al. The enduring effects of abuse and related adverse experiences in childhood. Eur Arch Psychiatry Clin Neurosci 256, 174–186 (2006). https://doi.org/10.1007/s00406-005-0624-4
3. Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The internet and child sexual offending: A criminological review. Aggression and Violent Behavior, 13, 216–228. https://doi.org/10.1016/j.avb.2008.03.007
4. van der Bruggen, M., Blokland, A. (2021). Child Sexual Exploitation Communities on the Darknet: How Organized Are They? In: Weulen Kranenbarg, M., Leukfeldt, R. (eds) Cybercrime in Context. Crime and Justice in Digital Society, vol I. Springer, Cham. https://doi.org/10.1007/978-3-030-60527-8_15
5. Childlight. (2024). Into the Light Index. https://intothelight.childlight.org/
6. Chopin, J., Fortin, F., & Paquette, S. (2022). Childhood victimization and polyvictimization of online sexual offenders: A developmental psychopathology perspective. Child Abuse & Neglect, 129, 105659. https://doi.org/10.1016/j.chiabu.2022.105659.
7. Cortoni, F., & Marshall, W. L. (2001). Sex as a coping strategy and its relationship to juvenile sexual history and intimacy in sexual offenders. Sexual Abuse: A Journal of Research and Treatment, 13, 27-43. https://doi.org/10.1023/A:1009562312658
8. Davy, D. AI-produced child sexual abuse material: Insights from Darknet forum discussions, WeProtect Alliance, (Lat updated 16 Jan 2025) available at: https://www.weprotect.org/blog/ai-produced-child-sexual-abuse-material-insights-from-dark-web-forum-discussions/
9. Dervley, R., Perkins, D., Whitehead, H., Bailey, A., Gillespie, S. & Squire, T. (2017). Themes in participant feedback on a risk reduction programme for child sexual exploitation material offenders. Journal of Sexual Aggression, 23(1), 46-61. https://doi.org/10.1080/13552600.2016.1269958
10. Dong, B., Morrison, C. N., Branas, C. C., Richmond, T. S., & Wiebe, D. J. (2020). As violence unfolds: A space–time study of situational triggers of violent victimization among urban youth. Journal of quantitative criminology, 36, 119-152;
11. Egyptian Child Law No. 126 of 2008.

12. Felitti, V. J., Anda, R. F., Nordenberg, D., Williamson, D. F., Spitz, A. M., Edwards, V.,... & Marks, J. S. (1998). Relationship of childhood abuse and household dysfunction to many of the leading causes of death in adults: The Adverse Childhood Experiences (ACE) Study. American Journal of Preventive Medicine, 14(4), 245-258.
13. Fogg, B. J. (2002). Persuasive Technology: Using Computers to Change What We Think and Do. Ubiquity, 2002(2). https://doi.org/10.1145/764008.763957
14. Gannon, C., Blokland, A.A.J., Huikuri, S. *et al.* Child sexual abuse material on the darknet. *Forens Psychiatr Psychol Kriminol* 17, 353–365 (2023). https://doi.org/10.1007/s11757-023-00790-8
30. Gannoni, A., Voce, A., Napier, S., Boxall, H., & Thomsen, D. (2023). Preventing child sexual abuse material offending: An international review of initiatives. Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2023-06/rr28_preventing_child_sexual_abuse_material_offending.pdf
16. Gubbels, J.; Assink, M.; Prinzie, P.; van der Put, C.E. What Works in School-Based Programs for Child Abuse Prevention? The Perspectives of Young Child Abuse Survivors. *Soc. Sci.* 2021, *10*, 404. https://doi.org/https://doi.org/10.3390/socsci10100404
17. Hupont, I., Tolan, S., Gunes, H. *et al.* The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems. *Sci Rep* 12, 10688 (2022). https://doi.org/10.1038/s41598-022-14981-6
18. Insoll, T, Díaz Bethencourt, E, Ovaska, A, Lahtinen, H-M & Vaaranen-Valkonen, N. (2024). Knowledge to Prevent Online Sexual Violence Against Children: Insights from a Survey of Child Sexual Abuse Material Offenders.
19. Insoll T., Ovaska A. & Vaaranen-Valkonen N. (2021). CSAM Users in the Darknet: Protecting Children Through Prevention (Suojellaan Lapsia ry. ReDirection Survey Report 2021). https://www.suojellaanlapsia.fi/en/post/csam-users-in-the-dark-web-protecting-children-through-prevention
20. IWF 2024 Report; What has changed in the AI CSAM landscape? available at: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/
21. Knack, N, Holmes, D, & Fedoroff, JP (2020). Motivational pathways underlying the onset and maintenance of viewing child pornography on the Internet. Behavioral Sciences & the Law. https://doi.org/10.1002/bsl.2450
22. Knack, N., Winder, B., Murphy, L., and Fedoroff, J. P. (2019). Primary and secondary prevention of child sexual abuse. International Review of Psychiatry 31, no. 2, 181–94. https://doi.org/10.1080/09540261.2018.154187
23. Suojellaan Lapsia, Protect Children ry. (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse
24. Lätth, J., Landgren, V., McMahan, A., Sparre, C., Eriksson, J., Malki, K., Söderquist E., Görts Öberg, K., Rozental, A., Andersson, G., et al. (2022). Effects of internet-delivered cognitive behavioral therapy on use of child sexual abuse material: A randomized placebo-controlled trial on the Darknet. Internet Interventions 30: 100–590. https://doi.org/10.1016/j.invent.2022.100590
25. Letourneau, E. J., Schaeffer, C. M., Bradshaw, C. P., Ruzicka, A. E., Assini-Meytin, L. C., Nair, R., & Thorne, E. (2024). Responsible behavior with younger children: results from a pilot randomized evaluation of a school-based child sexual abuse perpetration prevention program. Child maltreatment, 29(1), 129-141. https://doi.org/https://doi.org/10.1177/10775595221130737
26. Nurmi, J., Paju, A., Brumley, B.B. et al. (2024). Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. Sci Rep 14, 7849. https://doi.org/10.1038/s41598-024-58346-7
27. Portnoff, R., Simpson, M., Wang, R., O'Gorman, T., Polgar, D., Tweed, R., Cummings, R., Hallinan, P., Myers, M., Schaffer, M., Herrera, S., Issembert, B.B., Brooks, B., and Lalani, F. (2024) Safety by Design for Generative AI: Preventing Child Sexual Abuse. Thorn Repository. Available at https://info.thorn.org/hubfs/thorn-safety-by-design-forgenerative-AI.pdf

28. Quayle, E., & Taylor, M. (2002). Child pornography and the internet: Perpetuating a cycle of abuse. Deviant Behavior, 23, 331–363. https://doi.org/10.1080/01639620290086413
29. Rimer, J.R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. Child Abuse & Neglect, Volume 90, 2019, 160-173, https://doi.org/10.1016/j.chiabu.2018.12.008
30. Schippers, E. E., Hoogsteder, L. M., & de Vogel, V. (2024). Theories on the Etiology of Deviant Sexual Interests: A Systematic Review. Sexual Abuse, 0(0). https://doi.org/https://doi.org/10.1177/10790632241271308
31. Scourfield, J., Stevens, D. E., & Merikangas, K. R. (1996). Substance abuse, comorbidity, and sensation seeking gender differences. Comprehensive Psychiatry, 37(6), 384-392.
32. Seto, M. C. (2019). The Motivation-Facilitation Model of Sexual Offending. Sexual Abuse, 31(1), 3-24. https://doi.org/https://doi.org/10.1177/1079063217720919
33. Silovsky, J. F., Hunter, M. D., & Taylor, E. K. (2019). Impact of early intervention for youth with problematic sexual behaviors and their caregivers. Journal of Sexual Aggression, 25(1), 4-15. https://doi.org/10.1080/13552600.2018.1507487
34. Steel, C. M. S., Newman, E., O'Rourke, S., and Quayle, E. (2023). Lawless space theory for online child sexual exploitation material offending. Aggression and Violent Behavior 68 (2023) 101809. https://doi.org/10.1016/j.avb.2022.101809
35. Steely Smith, M., Ten Bensel, T., Brattin, T., and Lytle, R. D. (2018). All part of the process? A qualitative examination of change in online child pornography behaviors. Criminal Justice Studies 31(3):279.296. https://doi.org/10.1080/1478601X.2018.1492389
36. Stück, E., Briken, P. & Brunner, F. (2022). Changes in the risk of sexual reoffending: the role and relevance of perceived self-efficacy and adult attachment styles in correctional treatment. Sexual Abuse, 34(8), 891-922. https://doi.org/10.1177/10790632211054048
37. Suojellaan Lapsia, Protect Children ry. (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse
38. The Police Foundation. (2022). Turning the Tide Against Online Child Sexual Abuse. https://www.police-foundation.org.uk/wp-content/uploads/2022/07/turning_the_tide_FINAL-.pdf.
39. Webster E. M. (2022). The Impact of Adverse Childhood Experiences on Health and Development in Young Children. Global pediatric health, 9, 2333794X221078708. https://doi.org/10.1177/2333794X221078708
40. Wortley, R., Findlater, D., Bailey, A., & Zuhair, D. (2024). Accessing child sexual abuse material: Pathways to offending and online behaviour. Child Abuse & Neglect, 154, 106936. https://doi.org/10.1016/j.chiabu.2024.106936

A Digital Forensics Approach to Investigate Child Exploitation in the Dark Web



Ibtesam Mohamed Al Awadhi

1 Introduction

The exponential rise of cybercrime in the digital age has made things very hard for law enforcement, especially when trying to find illegal activities on the Dark Web. Exploitation of children is a very scary crime that is made easier by this anonymous online space. Because the Dark Web is anonymous and encrypted, criminals have much freedom to do what they want on it. This makes it hard for normal investigating methods to get into these secret networks. This chapter goes into great detail about the moral, legal, and technical problems that come up when you use digital forensics to look into people who abuse children on the Dark Web.

2 The Role of Digital Forensics in Cybercrimes

In the investigation of cybercrimes, digital forensics plays an important role by retrieving electronic and digital evidence by rules (Subektiningsih & Hariyadi, 2022). Digital forensics readiness (DFR) encompasses proactive measures aimed at effectively handling digital incidents, cybercrimes, and data breaches (Mahdi, 2024). Digital forensics encompasses a wide series of investigative methodologies specifically developed to tackle particular areas of scrutiny. Such approaches employ many methodologies, technology, and procedures. Memory investigation examines volatile memory (RAM) to gather evidence, identify malicious activities, and simulate cybercrime events (Mehmood, 2024). Forensic network analysis is the methodical surveillance, collection, documentation, and examination of data networks to identify security breaches, innovations, and assaults. Computer networks are implicated in the

I. M. Al Awadhi (✉)
Dubai police academy UAE, Dubai, UAE
e-mail: e.alawadi@dubaipolice.ac.ae

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_7

perpetration of multiple cybercrimes (George & Uppin, 2021). Mobile forensics examines data collected from mobile devices to discover pertinent digital evidence of investigative value (Ghannam 2018). Computer registries are essential in digital forensic investigations since they uncover evidence of cybercrimes, determine the time of crimes on computer systems, and identify user activities when the crimes occurred (Binjuraid & Din, 2018). The importance of digital forensics investigations in cybercrimes is in their ability to authenticate various crimes, provide location data, establish timeframes for events, and identify patterns in user behavior that are associated with suspicious and illegal activities (Miranda, 2020). According to Rakha (2024), a robust judicial system is the best way to fight cybercrime. Cybercrime is getting worse and more popular, and not many tools can help with it. The urge to fight hacking quickly makes digital forensics even more critical (Irons & Lallie, 2014). The application of digital forensics in addressing cybercrimes signifies notable progress in the field of cybersecurity. Alghamdi, 2021. Furthermore, it is crucial to establish consistent procedures, legislation, investigation approaches, and instructional initiatives for cybercrime investigators to efficiently tackle the difficulties faced in cybercrime investigations (Odoyo et al., 2020). At its core, digital forensics is important for looking into cybercrimes because it helps get evidence, analyze memory, use network forensics, and set up rules for how to deal with cybercrimes successfully. The most important things are to quickly find relevant proof and figure out how to deal with the complexity of cybercrime.

3 Legal and Ethical Considerations when Dealing with the Dark Web Investigation

(a) Legal Framework.

When doing investigations on the Dark Web, you need to think carefully about legal and moral problems to make sure you follow the law and protect both people's privacy and data protection rights. Davies (2020) states that the legislative framework regulating investigations on the Dark Web offers law enforcement authorities specific guidelines for the suitable methods and approaches to investigate and establish sanctions against persons involved in illicit activities on the Dark Web. Furthermore, this methodology enhances the demarcation of the boundaries of law enforcement jurisdiction on the Dark Web, especially when confronted with the difficulties posed by technologies that provide anonymity and encryption (Ghappour, 2016). This study aims to present a comprehensive survey of the commonly used frameworks for conducting investigations on the Dark Web. These frameworks include a variety of tactics that are meant to help law enforcement agencies do a better job of stopping crime on the Dark Web, which is an anonymous online space. The main goal of the MFScope system is to get information from the Dark Web, pull out information about cryptocurrencies, and look at how people use them. This way of thinking is especially helpful for questions about money transfers and cases of cryptocurrency

abuse (Lee et al., 2019). Furthermore, the OSIRT system is an invaluable instrument employed by law enforcement agencies in the UK to acquire website data, including videos, screenshots, and audit logs. According to Bergman and Popov (2023), its goal is to protect the evidence gathered from the Dark Web and keep the chain of control intact during investigations. This technology makes it easier to keep track of all digital proof, which is very important for legal proceedings. Moreover, the ANITA platform, introduced by law enforcement organizations, provides them with the essential resources to identify, examine, and alleviate illicit operations on the dark web. This is achieved via the automated surveillance, examination, and correlation of data, while preserving the chain of custody, which is crucial for carrying out thorough and legally valid investigations on the Dark Web (Mazzonello et al., 2021). The proposed targeted crawling technique provides supplementary features beyond the mere traversal of the Tor network. This methodology enables the exploration of both the Surface Web and other darknets within the Dark Web, such as I2P and Freenet, by considering the destination network type of a hyperlink and the surrounding local environment (Iliou et al., 2017). By using this method, more information can be gathered for studies. In conclusion, the MFScope framework, the OSIRT system, the ANITA platform, and the focused crawling method are all examples of frameworks that can help law enforcement agencies do investigations on the Dark Web better. These frameworks make it easier to keep evidence safe and allow for more thorough monitoring and analysis of illegal behavior in this hidden online space.

Hypothetical Case Study applying OSIRT and ANITA platforms. Employing OSIRT to Examine "ShadowTrade" Law enforcement commences an inquiry into "ShadowTrade," a Dark Web network enabling illicit drug transactions. Investigators utilize OSIRT to methodically collect open-source intelligence regarding the platform and its users. Applying OSIRT, they distinguish pseudonymous vendor profiles, monitor bitcoin wallets associated with transactions, and gather metadata from forums addressing ShadowTrade activities. OSIRT's capacity to archive web pages guarantees the preservation of evidence for legal actions. Subsequent investigation uncovers patterns of recurrent Bitcoin transactions directed to a particular wallet, associated with shipments monitored by intercepted postal records. Investigators subsequently utilize ANITA to monitor the network activities of alleged administrators. ANITA's uses sophisticated network traceback methodologies to identify IP addresses associated with the platform's command-and-control servers. The integration of OSIRT for intelligence acquisition and ANITA for network tracing results in the discovery and apprehension of ShadowTrade's operators. Evidence gathered through these frameworks facilitates successful prosecutions. Digital forensic tools and frameworks convert theoretical methodology into practical results to fight against Dark web crimes.

(b) Privacy and Data Protection.

The Dark Web's anonymity and encryption capabilities present ethical quandaries regarding privacy and data security within the framework of investigations. When these things are present, it can be hard to balance the needs of the investigation with people's right to privacy (Saleem et al., 2022). Police must be very good at finding

this fine line between protecting people's right to privacy and gathering evidence against hacking (Saleem et al., 2022). Furthermore, using pseudonyms and encrypted communication on the Dark Web raises ethical concerns regarding the privacy of persons engaged in legal activity on these networks (Goanta, 2020). In summary, the successful execution of Dark Web investigations necessitates a robust legal structure that grants direction to law enforcement endeavors inside the boundaries of the law. Adhering to ethical norms, especially with privacy and data protection, is essential for protecting the rights of individuals in Dark Web investigations.

Cross-border collaboration and jurisdictional obstacles are significant issues in Dark Web investigations, as the global nature of cybercrime takes advantage of discrepancies in legal frameworks, data protection regulations, and evidence management methods (Weng et al., 2019; Ghanem et al. 2023). International cooperation protocols, including those established by INTERPOL, Europol, and the Budapest Convention on Cybercrime, enable collaborative operations and data exchange; however, delays in acquiring cross-border evidence, varying levels of commitment, and geopolitical tensions may hinder advancement (Rajamäki, 2022; Yunelfi et al., 2022). Improving collaboration via standardized legal frameworks, robust collaborations, and collaborative training programs is crucial for effectively tackling these difficulties and dismantling Dark Web criminal networks (Zhang et al., 2022; Pizzolante et al., 2020).

4 Evidence Collection from the Dark Web

When performing investigations on the Dark Web, it is crucial to utilize tools and methodologies to retrieve pertinent content for investigation. Implementing a methodical strategy to digital investigation is of utmost importance. First and foremost, digital forensic specialists should employ automated techniques to collect data from the Dark Web, enabling the detection of illicit activities. The analysis was undertaken by Basheer and Alkhatib in 2019. Therefore, it is imperative to employ web crawlers to automatically retrieve web information from Dark Web sites, so simplifying the collection and protection of possible evidence for investigative objectives (Bergman & Popov, 2023). It is imperative to develop novel protocols, such as the D2WFP protocol, that may be employed to detect, extract, and analyzing activity on the Deep and Dark Web in order to gather data (Ghanem et al. 2023) securely. Implementing encryption techniques and anonymity tools is essential for practitioners to protect the identities of investigators and guarantee data security during evidence collection (Carminati & Ferrari, 2005). Furthermore, it is imperative to devise sophisticated methodologies to detect and analyze the hazards that arise from the Dark Web, so ensuring a proactive approach to collecting evidence (Nazah et al., 2020). Gain an understanding of the degree of anonymity provided by the Dark Web and its implications for preserving privacy and security in investigations, therefore enabling informed decision-making (Saleem et al., 2022). Achieve enhanced data collecting accuracy from Dark Web sources by employing sophisticated web

crawlers that have been fine-tuned and equipped with natural language processing capabilities (Sekhar et al., 2019). Comply with data protection regulations, such as GDPR, to ensure that user consent is obtained before collecting personal information during investigations (Fernandez et al., 2021). The research undertaken by Lee et al. (2019) has evidenced the ability to gather cryptocurrency addresses from the Dark Web, therefore enhancing our comprehension of illicit activities linked to cryptocurrencies. Bergman and Popov (2023) assert that Dark online crawlers have a vital function in autonomously collecting online metadata, therefore safeguarding material that may potentially serve as leads or evidence in investigative processes. The approach proposed by Hayes et al. (2018) provides a set of principles for carrying out studies of Dark Web marketplaces with more efficiency. It demonstrates how data from these platforms might be used to establish the identities of persons engaged in illicit activities. Thorough comprehension of the requirements of law enforcement is crucial while carrying out investigations on the Dark Web, as emphasized by (Goodison et al., 2019). A comprehensive grasp of this concept is essential in order to effectively tackle the challenges associated with collecting digital evidence from cloud service providers. Furthermore, the research undertaken by Basheer and Alkhatib (2021) underscores the significance of scrutinizing Dark Web content for the purpose of eliciting cyber threat intelligence, so facilitating the detection and mitigation of cybercrimes. The H2020 ANITA platform, as specified by Mazzonello et al. (2021), aims to equip law enforcement agencies with the essential resources to oversee and assess illegal activities carried out on the internet, namely on the Dark Web. The objective is to augment investigative endeavors by efficiently assisting law enforcement. To effectively combat cybercrimes, law enforcement agencies can improve their evidence collection, analysis, and intelligence-gathering capabilities by incorporating study findings and utilizing specialized tools and platforms specifically optimized for Dark Web investigations.

In Dark Web investigations, employing privacy-preserving approaches is essential for reconciling successful intelligence collection with the safeguarding of individual privacy rights. To protect investigator's identity and reduce privacy violations pseudonymous identities, zero-knowledge proofs, and homomorphic encryption are used (Weng et al., 2019; Ghanem et al. 2023). Secure, privately managed platforms and token-based monitoring augment data protection by separating sensitive information and concentrating solely on unlawful behaviors without direct data acquisition (Zhang et al., 2022; Arfeen et al., 2021). Moreover, ethical AI instruments and rigorous data minimization techniques provide the fast processing of extensive datasets while anonymizing extraneous information, so ensuring adherence to ethical and legal standards (Rajamäki, 2022; Pizzolante et al., 2020). These methods safeguard the privacy of uninvolved individuals while allowing law enforcement to reduce cybercrime effectively and ethically.

5 Digital Forensics Tools and Techniques

The application of digital forensics technologies and methodologies is essential in examining cybercrimes and recovering digital evidence. The development of these tools is driven by the necessity to combat cybercrimes and effectively outperform malefactors. Adams, 2024. The aforementioned techniques facilitate the detection of unlawful activities and improper conduct by the application of scientific methodologies and research frameworks (MbuguaChahira et al., 2016). Ongoing improvements in live forensic analysis methods are being developed to efficiently combat evolving criminal tactics and comprehensively investigate unlawful activities, therefore guaranteeing the fair dispensation of justice (Rahman & Khan, 2015). In the field of forensic investigations, web application forensics solutions offer efficient data analysis capabilities for web applications (Lazzez & Slimani, 2015). In order to enhance the efficiency and dependability of digital investigations, intelligent forensics integrates several approaches and technologies, such as social network analysis and artificial intelligence (Alghamdi, 2021). Specialized tools for conducting web browser forensic investigations include Autopsy, Browser History Examiner (BHE), and Net Analysis. Hunchly is a browser-based investigation tools designed to capture web pages and create searchable archive (Williams & Stephens, 2020). This tool is useful in dark web investigation to find documents. Hunchly allows automatic capture and save web pages, and could be access through Tor network. It can be used mainly to ensure that the evidences is preserved and organized for future analysis. CipherTrace is a specialized cryptocurrency investigation tool (Japinye, 2024). It is designed to trace blockchain transaction. This tool can facilitate tracking cryptocurrency transactions with illicit activities in the Dark Web. SpiderFoot is an open-source reconnaissance tool specifically gather intelligence across internet and the Dark Web (Carr et al., 2019). It mainly valuable for uncovering links, personal information, and domain details which are essential in any digital forensic investigation. These technologies facilitate the comparison of features and the examination of digital evidence by investigators (Ahmad et al., 2021). Self-organizing maps are used to detect anomalous behavior in digital investigations, supporting investigators in comprehensive analyses of digital crimes (Fei et al., 2006). Moreover, it is crucial to employ established protocols that depend on cutting-edge technology to maintain the precision and dependability of digital evidence and the findings of forensic investigations (Zareen et al., 2015). Furthermore, the utilization of software such as the NirSoft forensic tool and integrated conceptual digital forensic frameworks enables the retrieval of digital traces from cloud storage and the following implementation of forensic processing (Adesina et al., 2022). In cases of digital crime, forensic tools specifically developed for commercial use has the capacity to recover erased data, therefore assisting in the retrieval of crucial evidence (Umar et al., 2017). The utilization of mobile forensic technology is crucial in the analysis of smartphones and the extraction of incriminating evidence from mobile devices (Umar et al., 2018). Ultimately, the continuous advancement and use of digital forensic tools and techniques

are essential for effectively scrutinizing cybercrimes, recovering digital evidence, and upholding the integrity of forensic analyses.

The changing characteristics of the Dark Web require sophisticated technological and operational adjustments in the future of digital forensics to improve investigation efficacy. Incorporating AI and machine learning will facilitate the automatic detection of criminal tendencies and predictive analytics, while progress in blockchain forensics will tackle the difficulties of tracking privacy-centric cryptocurrencies such as Monero and Zcash. As quantum computing exposes current encryption methods, implementing quantum-resistant cryptography and enhancements to forensic tools for data decryption and analysis will be imperative. Decentralized platforms and blockchain marketplaces will require advanced surveillance technologies for peer-to-peer network research. Privacy-preserving techniques, including homomorphic encryption and zero-knowledge proofs, will guarantee ethical adherence and safeguard individual rights during inquiries. Future frameworks will improve cross-border collaboration via standardized protocols and real-time data sharing, tackling jurisdictional problems. Furthermore, immersive technologies such as VR and AR will induce forensics to modify their approaches to probing criminal actions in virtual settings. At the same time, IoT devices will need protocols for evidence extraction and analysis. Advanced anonymity evasion techniques, such as network traffic analysis and deanonymization, will facilitate the revelation of concealed identities on platforms like Tor, while real-time AI-driven surveillance tools will offer immediate alerts and ongoing monitoring of Dark Web activities, thereby enabling proactive law enforcement interventions.

6 Data Recovery, Data Carving, Encrypted Data, and Malware Analysis

An effective strategy for data recovery, data carving, encrypted data, and malware analysis entails the use of a wide array of tools and methodologies derived from several academic disciplines. In order to recover lost or damaged data, several data recovery methods can be employed, such as file header-based recovery, content-based recovery, and metadata-based recovery (Zhu, 2024). The Cauchy Coding (CaCo) technique, introduced by Zhang et al. Funde & Swain (2022), is employed for the purpose of encoding and decoding data, hence enhancing the retrieveability and security of data in networked storage systems (Funde & Swain, 2022; Hou, 2016). Cauchy matrices enhance data recovery and security in cloud systems (Hou, 2016; Mousavi et al., 2021). Cauchy matrices have been employed to enhance data retrieval through the identification and categorization of data (Mousavi et al., 2021). Cauchy codes have also been examined in the field of numerical relativity. Reisswig et al. (2010), Babiuc et al. (2009), and Handmer & Szilágyi (2014) have demonstrated that these algorithms have successfully extracted gravitational waves and resolved intricate physics difficulties. The extraction of gauge-invariant gravitational waves

from astrophysical simulations has been effectively achieved using Cauchy codes and characteristic extraction methods (Babiuc et al., 2009; Handmer & Szilágyi, 2014). The adaptability of Cauchy matrices in coding theory has been demonstrated by its application in the construct of MDS codes (Roth & Lempel, 1989; Mousavi et al., 2021). Word line interference-based data recovery methods are employed for the purpose of data carving. A study conducted by Huo et al. (2018) investigated logical data recovery techniques designed exclusively for USB devices. The research undertaken by Ravindra et al. (2013) is quite valuable. These methodologies enable the recovery of data from storage devices, even in situations when the file system structures are either damaged or non-existent. The analysis of encrypted data can be accomplished by employing specialized tools and methodologies that especially focus on data concealment strategies, such as the RGB-LSB mechanism (Agham & Pattewar, 2014). These methodologies are essential for recovering hidden or encrypted data within digital systems. Conducting malware analysis is a crucial component of cybersecurity, and there exist several approaches and technologies that can be employed for this objective. This paper by Bayer et al. (2006) specifically examines the dynamic analysis of hazardous code. Moreover, the investigation also includes the examination of stacking classifiers and dendrogram visualization methods. Nallabala (2024) serves as an example of techniques that can be used to analyze malware behavior, detect new variations, and enhance the identification of established malware lineages. In order to guarantee efficient and comprehensive investigations, it is imperative to utilize a range of specialized tools and techniques tailored for each individual work, including data recovery, data carving, encrypted data analysis, and malware analysis.

7 Case Studies and Examples

The examination of case studies and examples within the domain of digital forensics provides valuable perspectives on the practical implementations and challenges encountered. An illustration of a case study is the inquiry undertaken by (Chen et al., 2008), which centers on exposing the concealed elements of the Dark Web by scrutinizing the existence of Jihadist operations on the internet. The aim of this study was to assess the efficacy of methods in assisting terrorism analysts in obtaining and analyzing information from the Dark Web. By exploring the material and actions on the Dark Web, researchers can deepen their comprehension of illicit online behaviors and their hazards. A further relevant case study is the study undertaken by Alotaibi et al. (2022), which particularly investigates the domain of Computer Forensics and its implementation within the Dark Net Forensic Framework. In 2017, Interpol started the Blackwrist operation, it was a global operation that focused on the dark web's spread of child sexual abuse materials (CSAM) (Woodhams et al., 2021). The operation, which involved several nations, effectively disrupted a CSAM distribution network, which resulted in the arrest of important administrators and the rescuing of many children from exploitation. In April 2021, German authorities and Europol

successfully shut down "Bostown" which was a dark web platform that shared child sexual materials and had more than 400,000 registered users (Oosthoek et al., 2023). Many victims were identified, and many administrators were arrested. This operation identified the need for international collaboration in combating such crimes. The present paper investigates the methodologies and conceptual frameworks employed in the identification of digital evidence within the Dark Web. The study of computer forensics within the framework of the Dark Web enables researchers to develop effective methods for identifying and examining cybercrimes in hidden online environments. Rajamäki (2022) conducted a focused analysis of open-source intelligence (OSINT) on the Dark Web, focused primarily on investigations pertaining to child abuse material. This study emphasized the significance of using Dark Web resources to counter illicit activities and protect susceptible communities. Furthermore, Rochmadi's (2019) study on Live Forensics for Anti-Forensic Analysis on Web Browsers emphasizes a situation where illicit actors might exploit the advantages of web browsers to eliminate or diminish digital evidence. The importance of staying current with emerging forensic technologies is underscored in order to effectively address anti-forensic practices and ensure the integrity of digital evidence. Furthermore, Hayes et al. (2018) designed a case study to validate the efficacy of their proposed analytical methodology in examining Dark Web marketplaces. They emphasized the significance of employing systematic approaches to examine illegal behavior within the Dark Web environment. The offered case studies underscore the necessity of employing digital forensic tools, methodologies, and frameworks to effectively negotiate the intricacies of the Dark Web, enhance cybercrime investigations, and surmount obstacles posed by anti-forensic technology in the digital realm. Criminals on the Dark Web apply Anti-Forensics tactics like anonymity tools (e.g., Tor and VPNs), obfuscating techniques (e.g., steganography and file renaming), captcha bypasses, privacy-focused cryptocurrencies such as Monero and Zcash. All those methods obscure identities and hide illicit activities, and harden financial tracking (Weng et al., 2019). To counter these tactics, investigators need to utilize advanced traffic analysis techniques to identify any anti-forensic methods applied.

8 Challenges the Investigators Might Come across while Investigating

Undertaking digital forensics to probe cybercrimes poses investigators with a multitude of challenges. These concerns are highlighted in the literature and can significantly impact the effectiveness of research initiatives. Some significant challenges include the analysis of data stored in distant data centers, and the lack of physical access or control over the locations where the data is stored may make it impossible to examine decentralized data logs (Ahmad et al. 2021). The decentralized character of digital forensic evidence and the need to adhere to legal protocols for evidence

gathering could provide challenges in court proceedings, as specific evidence may be deemed exempt from admission (Brown, 2022). Establishing the sequence of investigative methods to employ can be challenging as each strategy requires time and effort, and investigators may lack knowledge of the methods already used before concluding the inquiry (Atefi et al., 2023). The process of investigating accidents in the Internet of Things (IoT) environment may be hindered by the wide range of systems and data, the vast amount of data created by IoT devices, and the fast pace at which data is generated (Koroniotis et al., 2019). Cybercriminals may employ anti-forensic techniques to eliminate or degrade digital evidence, therefore presenting challenges for investigators in their endeavors to effectively safeguard and assess evidence (Yaacoub, 2021). In the discipline of forensic science, standardization and research provide significant hurdles. The issues encompass the requirement for novel methods to expedite the collection and examination of evidence, adoption of unconventional techniques, and development of economical equipment for various forensic purposes (Harichandran et al., 2016). The validation and verification of forensic instruments include the implementation of comprehensive testing and validation procedures to guarantee their dependability and accuracy. Its objective is to ensure the integrity of the gathered and assessed evidence (Guo & Slay, 2010). An inherent challenge in utilizing cutting-edge forensic technologies during investigations is the absence of shared datasets for the purpose of evaluating these methods. Such lack of presence impedes their utility and restricts their acceptance (Luciano et al., 2018). The aforementioned issues underscore the complex character of digital forensic investigations and the imperative of addressing them in order to enhance the efficiency and reliability of electronic crime investigations.

9 Training and Skill Development

In order to effectively investigate cybercrimes, particularly those involving the Dark web and child abuse, professionals in the field of digital forensics must undertake training and skill development to gain the prerequisite knowledge and expertise. Numerous sources provide significant insights into training programs, skill development initiatives, and optimal strategies in this domain: 1. Casey, Eoghan. “Digital Forensics Education: Historical Overview, Current Status, and Prospects” (2017)—a comprehensive analysis of the evolution of digital forensics education is presented in this research, with a focus on the need of continuous learning and skill improvement in this rapidly evolving field. 2. Carrier and Spafford presented a book titled “Introduction to Digital Forensics: Exploring the Fundamentals.” The year 2003. This paper outlines the fundamental skills and knowledge required for individuals who want to pursue a career in digital forensics, providing a well-defined and methodical strategy for their training and skill development. 3. The book “Guide to Computer Forensics and Investigations” was published by Nelson et al. in 2016. This manual is a very valuable resource for anyone seeking to enhance their proficiency in computer

forensics and investigations. This resource offers pragmatic concepts and methodologies for training. 4. Sammons, the author of "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics" (2012), provides a comprehensive understanding of the fundamental concepts and methodologies of digital forensics. This book is highly recommended for both beginners and professionals seeking to bolster their knowledge in this field. 5. In their publication titled "Digital Forensics Education: A Review of Challenges and Solutions" (2020), Daryabar et al. undertook a thorough analysis of the obstacles and remedies in the domain of digital forensics education. This research paper investigates the difficulties faced in digital forensics education and proposes strategies to enhance training programs and initiatives for skill development. The cited sources offer valuable perspectives on the training and skill development environment in digital forensics, providing support for individuals aiming to enhance their abilities in this essential field. An essential element in successfully training staff in researching child abuse on the Dark Web is the adoption of a comprehensive strategy that integrates several instructional materials and methodologies. Drawing upon the following sources can provide valuable insights on developing tailored training programs for this specific goal: 1. The study undertaken by Pathirana and Zoysa (2015) investigated the effectiveness of a concise training program on child protection for police personnel in Sri Lanka. The aim of this program was to provide education concerning different aspects of child abuse, foster shifts in attitudes, and cultivate proficiency in performing forensic assessments. The aforementioned skills are crucial for the examination of cases involving child abuse, especially those that take place on the Dark Web (Pathirana & Zoysa, 2015). 2. Pathirana, Bashya, and Zoysa, Peter (2015). An evaluation of the efficacy of a brief training session on safeguarding children among police officers in Sri Lanka. The International Journal of Police Science & Management, volume 17, issue 3, pages 189–193. Citation: https://doi.org/10.1177/1461355715596507 3. Reiniger et al. (1995) emphasized the need of mandatory training for professionals to improve the practice of documenting suspected cases of child abuse. Training programs of this kind have the capacity to enhance the skills of those involved in child protection and investigation. Consequently, this results in a more effective and satisfactory management of instances related to child abuse, including those occurring on internet platforms like the Dark Web (Reiniger et al., 1995). 4. Robison, E., Reiniger, A., and McHugh, M. (1995). The implementation of compulsory training for professionals: a strategy to enhance the reporting of suspected child abuse. Child Abuse & Neglect, volume 19, issue 1, pages 63–69. Doi: 10.1016/0145-2134(94)00105-4 5. A study conducted by Solomon et al. (2016) investigated the impact of foster parent training on both parenting abilities and child disruptive behavior. Implementing streamlined training programs that prioritize the crucial and effective components will improve the accessibility and utility for individuals involved in child protection and investigation. This methodology provides users with the necessary skills to effectively manage instances of child abuse (Solomon et al., 2016). 6. Reference: Solomon, D., Niec, L., and Schoonover, C. (2016). The influence of foster parent training on the development of parenting skills and the management of child disruptive behavior. Journal of Child Maltreatment, 22(1), 3–13. The DOI for the article is 10.1177/1077559516679514.

The incorporation of the material from these sources into training programs enables individuals to acquire the requisite knowledge, skills, and attitudes necessary for conducting investigations on instances of child abuse taking place on the Dark Web. Implementing training programs that focus on forensic investigations, changes in attitudes, and effective reporting protocols can significantly contribute to combating child abuse and protecting vulnerable groups in online environments.

10 Collaboration and Information Sharing between Law Enforcement Agencies, Experts, and Digital Forensic Teams

The references show that collaboration and information sharing across law enforcement agencies, professionals, and digital forensic teams can be facilitated through various initiatives and strategies. Presented below are a few noteworthy observations: The research undertaken by Kebande et al. (2021) emphasizes the need of creating a Digital Forensic Readiness (DFR) repository that gathers digital evidence from many sources. This repository can be disseminated across different geographical areas and utilized by experts in the field of digital forensics and law enforcement organizations to enhance cooperation and the sharing of intelligence (Subektiningsih & Hariyadi, 2022). In their study, Casey and Zehnder (2020) outline the development of a digital forensic knowledge management system that facilitates the sharing of best practices and resources across law enforcement and intelligence agencies across various geographical areas. The main goal of this system is to enable the transmission of information and promote collaboration within the field of digital forensics (Mahdi, 2024). Plecas et al. (2011) highlight the significance of adopting evidence-based systems to enable the exchange of information among law enforcement organizations, especially in circumstances when security concerns are intensified and there is a greater requirement for cooperation between different authorities. Optimizing the distribution of information can enhance collaboration and yield more effective investigation outcomes (Mehmood, 2024). According to Azero (2024), it is crucial to foster collaboration among law enforcement agencies, academia, and the commercial sector in order to facilitate the exchange of knowledge and expertise. Engaging in such collaborations can enhance the combined ability to address cybercrime and sustain a competitive edge over malicious actors (George & Uppin, 2021). A study by Alghamdi (2021) demonstrates that the incorporation of artificial intelligence (AI) into digital forensics enables forensic professionals to perform digital forensic procedures in both reactive and proactive ways. By incorporating this system, the efficiency and effectiveness of digital investigations can be enhanced (Miranda, 2020). Bjelland and Vestby (2017) emphasize the strategic significance of multi-agency collaboration in augmenting the exchange of information among organizations, hence strengthening the efficacy of law enforcement efforts. Collaborative networks possess the

capacity to augment the intelligence sharing and improve the outcomes of investigations (Rakha, 2024). By leveraging these insights and constructing collaborative frameworks, law enforcement agencies, specialists, and digital forensic teams can enhance their collective capacity to effectively address cybercrime, facilitate information exchange, and foster collaboration.

11 Conclusion

Ultimately, digital forensics is essential in unraveling the intricacies of child exploitation on the Dark Web. As this chapter has shown, the complex technical obstacles presented by the Dark Web, together with the anonymity it provides to criminals, necessitate sophisticated forensic tools and investigation methods. The presented case examples exemplify the pragmatic implementations of these methodologies, while the discourse on legal and ethical constraints underscores the need of functioning within a comprehensive legal structure. Effective cooperation among law enforcement, forensic specialists, and international organizations is of utmost importance in addressing these worldwide criminal phenomena. Furthermore, continuous training and enhancement of skills are essential for investigators to maintain a competitive edge against ever-changing dangers. The proper utilization of digital forensics enables law enforcement to augment their ability to collect evidence, convict perpetrators, and ultimately safeguard vulnerable populations from exploitation.

References

Agham, V., & Pattewar, T. (2014, February). Data hiding technique by using RGB-LSB mechanism. In *International Conference on Information Communication and Embedded Systems (ICICES2014)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICICES.2014.7034000

Ahmad, A., Adamu, H., & Gambasha, S. (2021). Web browser forensic tools: Autopsy, BHE, and Net Analysis. *International Journal of Research and Innovation in Applied Science, 6*(5), 103-107. https://doi.org/10.51584/ijrias.2021.6506

Alghamdi, M. (2021). Digital forensics in cyber security—Recent trends, threats, and opportunities. *IntechOpen.* https://doi.org/10.5772/intechopen.94452

Alkhatib, B., & Basheer, R. (2019). Crawling the dark web: A conceptual perspective, challenges, and implementation. *Journal of Digital Information Management, 17*(2), 51-60. https://doi.org/10.6025/jdim/2019/17/2/51-60

Arfeen, A., Khan, M. A., Zafar, O., & Ahsan, U. (2021). Process based volatile memory forensics for ransomware detection. Concurrency and Computation: Practice and Experience, 34(4). https://doi.org/10.1002/cpe.6672

Babiuc, M., Bishop, N., Szilágyi, B., & Winicour, J. (2009). Strategies for the characteristic extraction of gravitational waveforms. *Physical Review D, 79*(8), 084011. https://doi.org/10.1103/PhysRevD.79.084011

Basheer, R., & Alkhatib, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications, 2021*, 1-21. https://doi.org/10.1155/2021/1302999

Bergman, J., & Popov, O. (2023). Exploring dark web crawlers: A systematic literature review of dark web crawlers and their implementation. *IEEE Access, 11*, 35914-35933. https://doi.org/10.1109/access.2023.3255165

Binjuraid, H., & Din, M. (2018). Case-based interpretation of Windows 10 registry forensics. *International Journal of Innovative Computing, 8*(1). https://doi.org/10.11113/ijic.v8n1.165

Brown, E. (2022). Digital forensic and distributed evidence. *Advances in Multidisciplinary & Scientific Research Journal Publication, 1*(1), 357-362. https://doi.org/10.22624/aims/crp-bk3-p57

Carminati, B., & Ferrari, E. (2005). Trusted privacy manager: A system for privacy enforcement. https://doi.org/10.1109/icde.2005.299

Carr, T., Zhuang, J., Sablan, D., LaRue, E., Wu, Y., Hasan, M. A., … & Mohler, G. (2019). Into the reverie: exploration of the dream market. 2019 IEEE International Conference on Big Data (Big Data), 1432-1441. https://doi.org/10.1109/bigdata47090.2019.9006092

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark web: A case study of jihad on the web. *Journal of the American Society for Information Science and Technology, 59*(8), 1347-1359. https://doi.org/10.1002/asi.20838

Davies, G. (2020). Shining a light on policing of the dark web: An analysis of UK investigatory powers. *The Journal of Criminal Law, 84*(5), 407-426. https://doi.org/10.1177/0022018320952557

Fei, B., Eloff, J., Olivier, M., & Venter, H. (2006). The use of self-organizing maps for anomalous behavior detection in a digital investigation. *Forensic Science International, 162*(1-3), 33-37. https://doi.org/10.1016/j.forsciint.2006.06.046

Fernandez, C., Chatzopoulos, D., Papadopoulos, D., & Hui, P. (2021). This website uses nudging: MTurk workers' behaviour on cookie consent notices. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW2), 1-22. https://doi.org/10.1145/3476087

Funde, S., & Swain, G. (2022). Data recovery approach with optimized Cauchy coding in distributed storage systems. *International Journal of Advanced Computer Science and Applications, 13*(6). https://doi.org/10.14569/ijacsa.2022.0130675

George, G., & Uppin, C. (2021). A proactive approach to network forensics intrusion (Denial of Service flood attack) using dynamic features selection and convolution neural network. *Open Journal of Physical Science, 2*(2), 1-9. https://doi.org/10.52417/ojps.v2i2.237

Ghanem, M. C., Mulvihill, P., Ouzzane, K., Djemai, R., & Dunsin, D. (2023). D2wfp: a novel protocol for forensically identifying, extracting, and analysing deep and dark web browsing activities.. https://doi.org/10.20944/preprints202308.0826.v1

Ghannam, H. A. (2018). Forensic analysis of artifacts of giant instant messaging "WhatsApp" in Android smartphone. *Journal of Applied Information, Communication and Technology, 5*(2), 63-72. https://doi.org/10.33555/ejaict.v5i2.55

Ghappour, A. (2016). Searching places unknown: Law enforcement jurisdiction on the dark web. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2742706

Goanta, C. (2020). The private governance of identity on the silk road. *Frontiers in Blockchain, 3*. https://doi.org/10.3389/fbloc.2020.00004

Goodison, S., Woods, D., Barnum, J., & Kemerer, A. (2019). Identifying law enforcement needs for conducting criminal investigations involving evidence on the dark web. *RAND Corporation*. https://doi.org/10.7249/rr2704

Handmer, C., & Szilágyi, B. (2014). Spectral characteristic evolution: A new algorithm for gravitational wave propagation. *Classical and Quantum Gravity, 32*(2), 025008. https://doi.org/10.1088/0264-9381/32/2/025008

Hayes, D., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information, 9*(8), 186. https://doi.org/10.3390/info9080186

Hou, H. (2016). Cauchy MDS array codes with efficient decoding method. https://doi.org/10.48550/arxiv.1611.09968

Iliou, C., Kalpakis, G., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2017). Hybrid focused crawling on the Surface and the Dark Web. *EURASIP Journal on Information Security, 2017*, 1-13. https://doi.org/10.1186/s13635-017-0055-5

Irons, A., & Lallie, H. (2014). Digital forensics to intelligent forensics. *Future Internet, 6*(3), 584-596. https://doi.org/10.3390/fi6030584

Japinye, A. O. (2024). Integrating machine learning in anti-money laundering through crypto: a comprehensive performance review. European Journal of Accounting, Auditing and Finance Research, 12(4), 54-80. https://doi.org/10.37745/ejaafr.2013/vol12n45480

Lazzez, A., & Slimani, T. (2015). Forensics investigation of web application security attacks. *International Journal of Computer Network and Information Security, 7*(3), 10-17. https://doi.org/10.5815/ijcnis.2015.03.02

Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., & Shin, S. (2019). Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web. *Proceedings of the 2019 Network and Distributed System Security Symposium.* https://doi.org/10.14722/ndss.2019.23055

Luciano, L., Baggili, I., Topor, M., Casey, P., & Breitinger, F. (2018). Digital forensics in the next five years. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* https://doi.org/10.1145/3230833.3232813

Mahdi, M. (2024). Proof of concept of a digital forensic readiness cybercrime language as a service. *International Conference on Cyber Warfare and Security, 19*(1), 191-199. https://doi.org/10.34190/iccws.19.1.2059

Mazzonello, V., Mattina, E., Acquaviva, R., Cina, G., Tommaso, M., Youssef, B., & Simoncini, S. (2021). The H2020 ANITA platform: Generating knowledge about crime through user-centred innovative tools. *Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI).* https://doi.org/10.1109/csci54926.2021.00178

Mehmood, R. (2024). Volatile data acquisition and analysis by using memory forensics techniques. *International Journal

Oosthoek, K., Staalduinen, M. v., & Smaragdakis, G. (2023). Quantifying dark web shops' illicit revenue. IEEE Access, 11, 4794-4808. https://doi.org/10.1109/access.2023.3235409

Pizzolante, R., Castiglione, A., Carpentieri, B., Contaldo, R., D'Angelo, G., & Palmieri, F. (2020). A machine learning-based memory forensics methodology for tor browser artifacts. Concurrency and Computation: Practice and Experience, 33(23). https://doi.org/10.1002/cpe.5935

Rajamäki, J. (2022). Osint on the dark web: child abuse material investigations. Information &Amp; Security: An International Journal, 53, 21-32. https://doi.org/10.11610/isij.5302

Weng, H., Zhao, B., Ji, S., Chen, J., Wang, T., He, Q., … & Beyah, R. (2019). Towards understanding the security of modern image captchas and underground captcha-solving services. Big Data Mining and Analytics, 2(2), 118-144. https://doi.org/10.26599/bdma.2019.9020001

Williams, J. and Stephens, P. (2020). Analysis of the 'open source internet research tool': a usage perspective from UK law enforcement. IFIP Advances in Information and Communication Technology, 341-352. https://doi.org/10.1007/978-3-030-57404-8_26

Woodhams, J., Kloess, J. A., Jose, B., & Hamilton-Giachritsis, C. (2021). Characteristics and behaviors of anonymous users of dark web platforms suspected of child sexual offenses. Frontiers in Psychology, 12. https://doi.org/10.3389/fpsyg.2021.623668

Yunelfi, P. R., Purwanto, Y., Ruriawan, M. F., Popalia, A. S., & Fahrani, F. (2022). Darkweb crawling using focused and classified algorithm. [CEPAT] Journal of Computer Engineering: Progress, Application and Technology, 1(02), 1. https://doi.org/10.25124/cepat.v1i02.4879

Zhang, N., Ebrahimi, M., Liu, W., & Chen, H. (2022). Counteracting dark web text-based captcha with generative adversarial learning for proactive cyber threat intelligence.. https://doi.org/10.48550/arxiv.2201.02799

The Child Offender and Victim on the Darknet: A Case Study 2



Mohammad Elhady Abdelhakiem Ratib Abdelhafiz

1 Introduction

Borders could no longer separate between people as they were in ancient times. Electronic communication has become a feature of the era, especially with the development and diversification of Internet uses and the emergence of social networking sites. It has become available for everyone to use the internet, access its sites, and create accounts to communicate with others. Communication is not limited to adults only, but is also used by children of almost all ages.

It is no longer limited to ordinary users. These advancements are not away from criminals, who spare no effort in taking advantage of every technology and development in committing their crimes, especially with the emergence of the darknet. The darknet is distinguished by the fact that it cannot be accessed through regular browsers, but rather through browsers that cannot be tracked or monitored.

This was combined with the emergence of Bitcoin, whose data and source cannot be tracked either. Bitcoin is the basic currency of the dark web and is the unit of account for dark web transactions, and through it, illegal transactions can be carried out, such as drugs and weapons trafficking, child pornography, violent videos, prostitution, hired killers, etc. (Kassab & Rosen, 2019, pp. 2 & 160).

Children are the most vulnerable to deviance. They easily fall into clutches and quagmire of crime, whether as perpetrators or victims. The case under study is the best example, in which the accused inciter was a child, and the victim was also a child.

States are working hard to confront cybercrimes as well as crimes across national borders. Many agreements have been concluded in this regard, such as the United Nations Convention against Transnational Organized Crime and the Arab Convention

M. E. A. R. Abdelhafiz (✉)
Dubai Police Academy, Dubai, UAE
e-mail: dr.melhady@dubaipolice.ac.ae

Faculty of Law, Assiut University, Assiut, Egypt

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_8

against Transnational Organized Crime. States also amend internal laws, in particular criminal laws, to combat that type of emerging crimes.

However, there are no specific provisions in either national criminal law or international agreements that address dangers of the darknet and criminalize illegal acts committed through it, despite its extreme dangerousness that is targeting children in particular.

The research aims, in its study of the present case, to investigate adequacy and extent of Egyptian criminal law as well as the international and regional agreements that Egypt has joined to confront this category of darknet cybercrimes, and then, to propose appropriate combating solutions and procedures.

2 Preliminary Issues

2.1 Background and Case Facts

The heinous crime was reported in April 2024. It had been occurred in many places, including mainly Kuwait, Egypt, and many other unknown states that have not been revealed by investigations yet.

The first defendant, an Egyptian child over 15 years old residing with his family in Kuwait, used the internet to contact the second defendant, an adult Egyptian man who works as a coffee shop waiter and resides in Egypt. The first defendant, the child, incited the second defendant, the adult, to kill a child, dismember, and mutilate the dead body, and film the whole operation in livestream, for five million Egyptian pounds in return.

The investigations proved that the first defendant committed the acts of communication and incitement while he was in Kuwait using a mobile phone with a SIM card owned by his father.

The inciting child had deceived the second defendant, the adult, made him to believe that the reason for dismembering the corpse was to use the body parts in human organ trafficking. While the fact was that the first defendant, the child, did so to broadcast these clips via the darknet and gain profits for himself.

In order to carry out the crime, the second defendant met the victim, a 15-year-old Egyptian child, and took him to an apartment he had rented in the Shubra district in Qalyubia city. Then the offender slaughtered the victim child. He then mutilated the corpse and removing internal organs and placed the viscera in a plastic bag. The killer had filmed the crime. Investigations revealed that the second defendant had previously sold his own kidney for a sum of money. He then committed this crime to obtain money.

Although the killer had committed the murder in all details and steps demanded by the inciter, the inciter child refused to send the money to him. The child inciter had procrastinated and asked the killer adult to repeat the process with another child to gain the money.

The crime was discovered as the dead body was found by the landlord lady. She immediately reported the crime and notified the Egyptian authorities.

The International Cooperation Office of the Public Prosecution and Interpol, in cooperation with the Kuwaiti authorities, played a major role in arresting the defendant and his father, deporting them from Kuwait to Egypt, and seizing all electronic communication devices, including cell phones and computers.

The accused child confessed that he did so in order to keep recorded video clips for broadcasting through the darknet. He also confessed that he committed similar crimes before. Upon examining the electronic devices, similar video clips were found that the accused was promoting via the darknet. The locations where they were filmed are not verified yet. The father of the accused child denied knowing or having any connection to the whole matter.

As there are no medical devices or equipment indicating that the victim's organs were to use for medical purposes as organ trafficking material, that indicates the real purpose of crime. The purpose of the crime was not to trade human organs, but rather, as the instigator child confessed, the purpose of the crime was sadistic murder, with the crime being recorded in video clips contain cruel, brutal, terrifying, and sadistic scenes being broadcast later via the darknet.

It was also proven during the investigations, through examining the seized mobile phones and electronic devices, that there were messages and communications proving that the first accused child incited another woman from Port-Said city to kill her 8-year-old son. The authorities were able to identify the woman, arrest her, and seize the electronic devices in her possession. When confronted and interrogated, the woman confessed to communicating with the child instigator through social media, where he asked her to kill her son. The accused woman actually drugged her son and filmed the act as if she was killing her son, to make the instigator believes that she had killed her son without actually intending to do so. The drug dose was excessive, which resulted in her son being transferred to a hospital to receive medical care until he regained consciousness. When the woman asked the first accused, the child instigator, to give her the agreed-upon sum of money, he refused and asked her to commit another murder.

The heinous crime was registered in the investigation files under Case No. 1820 of 2024, Administrative Section 1, Shubra El-Kheima. It was referred to the criminal trial under Case No. 9800 of 2024, Felonies Section 1, Shubra El-Kheima.

The case involves other defendants. Such as a pharmacy delivery man who had provided the principal killer with the drugs and medications he used to anesthetize the child victim before killing him. It also involves a broker for human organs who had mediated the sale of the killer's kidney in the past. It has not been proven with certainty whether these two defendants knew or engaged in the present crime or not (Alshorouk and Almasryalyoum newspapers, 2024).

2.2 Case Issues

The case raises many legal issues, some of which are objective and others are pertain to criminal procedures.

Among these objective issues are the crime of premeditated murder and malice aforethought, premeditated murder for hire, mutilation of the corpse, and participation in premeditated murder, especially electronic incitement via the internet. The case also raises debates about cybercrimes and darknet crimes, such as broadcasting violent clips that represent real crimes. The question also arises about whether the crime represents one of the acts of human trafficking or not?

The case also raises some issues related to criminal procedures such as the jurisdiction, both territorial and subject matter jurisdiction.

Regarding the fact that the accused inciter and the victim are counted as children, procedures of investigation and trial are special ones. The first defendant, who is an accomplice by incitement, as well as the victim, are both children according to the provisions of Egyptian law. A child according to the provisions of the law is anyone who has not exceeded 18 full Gregorian years of age, according to the International Convention against Transnational Organized Crime and its supplementary protocols, and Article 80 of the Egyptian Constitution and Article 2 of the Child Law. In defining what is meant by a child, Article 80 of the Constitution stipulates that a child is anyone who has not reached the age of eighteen. While Article 2 of the Child Law stipulates that a child is anyone who has not exceeded the age of 18 years (Abdeltawab, 1997, p. 24.).

Given the difference in wording between provisions of the constitution and the statute, we find that the statute provides more effective protection than the constitution. For defining a child, the statute considers anyone that "does not exceed" the age of 18 years, while the constitution refers to anyone who "does not reach" the age of 18 years. This means that anyone at the age of 18 years is protected as a child under the statute unlike the constitution.

2.3 Applicable Legal Rules

As the facts represent a transnational case, some international and regional criminal agreements can be relied upon, such as the United Nations Convention against Transnational Organized Crime, UNTOC, and protocols thereto, in particular The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children.

National criminal legal rules can also be applied in Egypt. These include the Penal Code of Egypt, PCE, the Criminal Procedure Code, CPCE, Child Laws, Cybercrimes Law, and Anti-Human Trafficking, AHT Law.

In general, although the investigations did not reveal yet whether an organized criminal group was behind the crime or not, provisions of the UNTOC can be relied

upon to clear some of issues raised by the case, in addition to rules of Egyptian legal framework.

3 Substantial Issues

*3.1 External Element (*Actus Reus*)*

3.1.1 Criminal Conduct

This crime had included many complicated acts, for example, the act of murder, then dismembering the body, filming it, and broadcasting the video clips, and before all that, there was incitement and agreement to carry out the murder for hire and filming it in preparation for broadcasting it via the darknet.

On the other hand, the crime is considered a transnational crime. According to Article 3 of the UNTOC, the crime is considered transnational when it is committed in more than one state; committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; or has substantial effects in another State. whether in the planning and preparation phase or the extension of its effects (Boister, 2016, pp. 134–135). This is typically applies to the case under investigation, which was incited and planned in Kuwait while the crime was committed in Egypt, although there is no evidence refers to the organized nature of the crime.

International agreements to combat transnational crimes usually depend on two very important elements. The first is setting general guidelines for the criminal behavior specific to each crime. The second is related to the impact of national law.

A convention combatting transnational crimes usually sets criminal rules and requires national courts to apply them. That application is viewed through the extent of necessity to relying upon national legal rules. Examples of these national rules include, inter alia, the requirement of criminal intent, defense to criminal liability, rules of attempt and criminal participation, etc. England and Wales Court of Appeal rules in *R v Safi and ors* (2003), according to that principle. The English court stated that the defense of duress is valid in applying the Aviation Security Act of 1982, which relies on rules of the Hague Hijacking Convention (Boister, 2022, p. 125).

The question arises about the extent to which the general rules of criminal law could be applied to what the agreement does not address. This matter usually existed because international criminal agreements usually focus on specific criminal acts without often addressing the general rules of criminalization and punishment, which may differ from one state to another.

Boister (2022) points to that matter by citing the example of German law, which does not punish for acts subsequent to a serious crime, if those acts are related to it, as if they were complementary to the criminal project and linked thereto (pp. 125–126).

That principle of German law is the same in Egyptian criminal law, while in other jurisdictions such principle is not applied.

Apply such principle to the case under study, we would find, for example, that acts of mutilation, filming, and broadcasting on the darknet are subsequent and complementary to the original criminal project, which is premeditated murder for hire. Such subsequent acts might be considered, for example, aggravating circumstances in certain jurisdictions, Iraqi law for instance, Articles 405 et seq. of Iraqi Penal Code (Saloom, 2009, p. 36). While in other states, these acts might be counted as independent crimes, such as crimes of corpse abuse or crimes of concealing a dead body.

3.1.2 Criminal Attempt

To analyze the external element of that type of crime, we should have a look at the criterion of attempt. It is the commencement of an execution with the intent to commit a felony or a misdemeanor, if completion thereof has been interrupted or failed due to circumstances beyond the offender's control (Hosny, 1989, pp. 344 *et seq.*). The question is about when is the perpetrator considered to have commenced execution? And how is the criterion of the essential step toward committing the crime applied?

The act has to be more than mere preparatory to the commission of the offense (Carr & Johnson, 2013, pp.143–145; Card, 2012, p. 592). However, there is no precise distinction between what is considered a mere preparation and what is counted as an attempt (Fletcher, 1998, p.176). For differentiation, courts adopt that the act could be punishable as attempt if there's a sufficient evidence that the perpetrator stepped an essential step out from the area of preparation into the area of execution (Card, 2012, p. 602; Elliott & Quinn, 2016, p. 278).

As Fletcher (1998) states, "If there was no reason to wait until the harm occurred, there was no reason to wait until the harm was "about" to occur. Better to catch the potential offender before he or she has a chance to get too close to a successful crime" (p. 172).

Accordingly, in darknet crimes, merely communicating with the child should be considered an attempt, that the perpetrator has thus moved from the area of preparatory acts to the area of initiating execution, if the purpose of such communication is to commit a crime and victimizing the child. In such regard, it is also possible to criminalize the attempt and impose the penalty of completed offense on the attempt in order to achieve complete protection for children.

In the same context, Dolliver and Poorman (2018) state that "cybercrimes are also not an "equal opportunity" offense. It is not possible to be a cyber offender without having access to cyberspace; however, one can become a victim of cybercrime without ever logging on to the Internet" (p. 156). And that exactly what happened in the case under investigation regarding the murdered victim.

In the USA, a bill was submitted to ban the darknet. The bill defined darknet as parts of the internet contain hidden sites or services that cannot be reached through normal search engines and tools, and can only be accessed using special tools or

means that hide identities and locations of users. The bill mainly aims to impose penalties on acts of using darknet for purposes of promoting controlled substances, such as drugs for example (S.1728—Dark Web Interdiction Act of 2023, 118th Congress).

3.1.3 Acts of Human Trafficking

According to criminal provisions against human trafficking, case facts represent human trafficking. The criminal behavior had been committed by exploiting the child victim in the most heinous form, which is murdering him with using deception and luring, filming the process and broadcasting on darknet for financial gain.

The criminal conduct is a practice similar to slavery and servitude, although the Egyptian law does not specify exclusive forms of behavior or exploitation. Article 2 of the AHT Law criminalize and form of trafficking, trading, or exploitation, noting that removing human organs and tissues, which is a form of human trafficking, was done in the case in the course of mutilation process and not for medical or scientific purposes. As the Public Prosecution stated that upon examining the crime scene, no medical equipment or tools were found, indicating that the purpose of removing the victim's internal organs was not for the purpose of using them in organ transplantation or medical experiments.

3.1.4 Criminal Participation

In general, criminal participation might be primary or secondary. Primary or principal participation is committed by an act that plays a major role in committing the crime, as if it is part of the criminal behavior. While secondary criminal participation, or complicity, it is made by an act that has a secondary role in the crime, such as incitement, agreement, or assistance, provided that the act of complicity results in the commission of the crime.

In certain jurisdictions, complicity is brought about by agreement or criminal conspiracy, if more than one criminal agrees to commit the crime. They are convicted of conspiracy even if the crime per se that they agreed to commit has not been consummated not commence the execution thereof, as long as they have committed an act that indicates the final intention to perpetrate the crime, as if the conspirators to rob a bank steal a car to commit the bank robbery (Bergman, 2020, p. 62).

According to criminal law of Egypt, agreement as a method of complicity is punishable only if the principal crime has been consummated upon that agreement, whether in the form perfect or attempted crime. This is based on the ruling of the Supreme Constitutional Court (No. 114/21, 2001) that invalidated Article 48 of the Penal Code, which had imposed punishment for criminal agreement regardless criminal result occurred thereupon.

Regarding the case, the inciter child was in Kuwait as he had incited the principal adult offender to murder a child victim for money. For the inciter child to be held

liable, a strong connection must be established, and proven, between the act of incitement and commission of the crime (Elliott & Quinn, 2016, p. 309), to prove that the inciter had persuaded the adult principal to commit murder (Jefferson, 2013, p. 169).

That principle is referred to as the test of "but-for," as if there is no incitement the crime would not have been committed (Kadish et al., 2022, p. 689). By applying the test, we can decide that if the child had not incited the principal offender, the later would not commit the murder nor mutilate corpse of the victim child.

Actually, we could address two significant points. The first is regarding murder for hire, and crime for hire in general, which could be considered the strongest forms of incitement and the most obvious examples of implementing the "but-for" test. Legislators should impose harsher penalties for offenders in crimes for hire. However, Egyptian criminal law counts financial gain in such cases as a motive, and does address crimes for hire in the same way as other forms of incitements.

The second point is related to the inciter's will, and how he could control and unleash the principal offender. As jurists stipulate that the act of incitement entails and indicates superiority of inciter's will over that of principal offender, while in cases of criminal agreement, the criminal wills are equal to each other (Awad, 1978, p. 247; Hosny, 1989, p. 439).

In the same context, although criminal laws punish accomplice as principal viewing them in the same area (Roach et al., 2020, p. 526), some jurists state further that the inciter is the mastermind. The inciter should be viewed as the principal perpetrator, not merely an accomplice. According to them, incitement is usually the work of masterminds that play behind the scenes and are considered more dangerous than the physical perpetrator of the crime, who works as a tool in the inciter's hands (Sedky, 1986, p. 357).

In viewing facts of the case, it is remarkable that the child's will, who is not fully capable according to law, was superior to adults' wills, the principal murderer and the woman he had instigated to murder her own son. Furthermore, the inciter had deceived adult offenders and refused to send money after finishing their criminal projects.

Notably, Article 116 *et seq.* of the Egyptian Child Law criminalizes the conduct of inciting a child to commit illegal acts by any means, including the use of a computer, considering that is what typically and usually happens, adults incite and deceive children to commit crimes, not vice versa.

The last point is regarding the inciter's father. In the case under investigation, the father would be liable for complicity by assistance, if it is proven that he was deliberately involved in making means of communication available for use in the manner in which they're used.

*3.2 Internal Element (*Mens Rea*)*

3.2.1 An Intentional Crime

Crimes require internal elements to be consummated, and cybercrimes are no exception. Internal element of an intentional crime is composed of knowledge and will (Boister, 2022, p. 127). For example, it is required that the perpetrator knows that he is committing the crime via the internet, and knows the age of the victim.

The question is about the extent to which the accused is supposed to know the age of the victim. This issue could be answered with regard to national criminal laws, but it is not always the same answer in cases of darknet crimes, and cybercrimes in general, whereas the other party of crime—the victim—is usually unknown personally to the perpetrator.

On the other hand, well-known traditional Internet sites provide conditions for use, including confirming the user's age, while that feature is not expected to be available in darknet sites, which are based primarily on anonymity and concealing users' identities.

However, it is logic to apply the same rule as in traditional crimes, and establish a presumption regarding perpetrator's knowledge of the victim's age, based on the fact that perpetrators accessed the darknet sites knowing about, and even seeking for, anonymity thereof.

In the case, we can note that the offenders were aware of the victim's age. Furthermore, the inciting child had stipulated the crime to be committed against a child.

Moreover, the *mens rea* can also be viewed from another angle. The internal element, as a personal element, means that the crime might be occurred even if no criminal result has been achieved as long as the perpetrator was willing for that result to occur and intended to cause it from the beginning.

An example of this can be given by criminalizing the perpetrator's mere access to the internet, whenever such access was for the purpose of committing a crime against children and minors, as well as in the case of criminalizing mere access to the darknet even if it was not accompanied by any criminal purpose.

The last point regarding internal element of the crime is related to premeditation. Premeditation refers to thinking about forehand, i.e., the final intent to commit the crime, as the offender contemplates and measures forethought and planning. Premeditation is considered an aggravating circumstance according to Articles 230–231 of the PCE (Hosny, 1981, p. 72; Ramadan, 1969, p. 253; Dressler, 2015, p. 64).

3.2.2 A Non-intentional Crime

Darknet cybercrimes are usually committed in intentional manner, i.e., *mens rea* therein takes the form of criminal intent. Nevertheless, they might be consummated in an intentional manner, as if the law criminalizes inciter's father for negligence in

parenting and observing his child, to the point where he was able to communicate many times, according to his statements, and commit many incitements, each of which takes a relatively long time, which indicates that negligence is almost proven against the father.

In general, criminal laws punish for mistreating children. They also criminalize non-intentional forms of such mistreatment, such as failure to provide a child with adequate care and contributing to the child's deviation, even unintentionally, as a father uses drugs in front of his children. That father is considered to have committed the crime even if the child does not use drugs (Bergman, 2020, pp. 60–62).

3.3 The Punishment

3.3.1 Primary Penalties

Based on crime facts, the crime is counted as a premeditated murder, followed by mistreating the corpse by mutilation, dismemberment, and audio-visual recording and filming the whole operation. According to Article 12 of the PCE, the crime is considered a felony (Sedky, 1986, pp. 202–203), as murder with premeditation is punishable by death penalty, Article 230 of the PCE (Hosny, 1981, p. 80; Ramadan, 1969, p. 255).

However, the court still has the right to reduce the penalty by one or two degrees in accordance with the right of clemency stipulated in Article 17 of the PCE, as the court might impose imprisonment for life or aggravated imprisonment instead of death penalty (Hosny, 1989, pp. 823–824).

As a general rule, when court chooses a penalty of aggravated imprisonment between usual limits that are 3–15 years according to Article 14 of the PCE (Hosny, 1989, pp. 724–725), but the minimum limit in the case has to be doubled, i.e., the penalty of aggravated imprisonment would become 6–15 years, as Article 116 bis of the Child Law stipulates that the minimum penalty stipulated for any crime committed by an adult against a child shall be doubled.

Furthermore, the crime is considered a serious crime in terms of UNTOC. Article 2b of the UNTOC defines a serious crime as that means conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or more severe penalty.

For the child inciter, the general rule in Egyptian law is that whoever participates in a crime shall be punished therefor, according to Article 41 of the PCE (Sedky, 1986, p. 353). Therefore, the accused child is liable for the same penalties as the adult murderer. However, since the inciter was a child at the time of committing the criminal behavior, he would be liable for special punitive measures in accordance with the Child Law of Egypt.

Actually, jurisdictions usually treat accused children by measures and penalties different from that imposed on adults (Hosny, 1989, pp. 944 *et seq.*) for example, death penalty and life imprisonment shall not be imposed on accused children (Marcus &

Wilson, 2016, p. 175). Article 111 of the Child Law imposes imprisonment, within its regular limits 3–15 years, instead of death penalty for accused child whose age exceeds 15 years old, with the possibility of applying clemency according to Article 17 of the PCE (Elgharib, 1994, pp. 1315–1317).

3.3.2 Accessory Penalties

When the court issues a primary penalty of a felony, accessory penalties are imposed by the virtue of law, Articles 24–25 of the PCE. Accessory penalties include, inter alia, deprivation of some rights and benefits, such as dismissal from public office if the convicted is a public employee, and placing the convicted under probationary police supervision after release (Surour, 1981, p. 751 *et seq.*).

3.3.3 Complementary Penalties

Confiscation is usually imposed as a complementary penalty for property used for or obtained from committed crime, including tools used for committing the crime, such as cell phones, laptops, etc. That property is counted as proceeds of crime according to the definition of the aforementioned UNTOC, therefore, it is subject to forfeiture and seizure in preparation for confiscation according to Article 12 of the Convention (Boister, 2016, p. 145), and Article 30 of the PCE (Surour, 1981, p. 767 *et seq.*).

3.3.4 Comments Regarding the Punishment

Given the facts of the case, some personal characteristics and traits of the criminals are obvious, and might be useful in individualizing the punitive implementation regarding these criminals.

For example, the second accused—the murderer—had previously sold his own kidney, that indicates his criminal tendencies to the point that he did not care about selling his own organs and risking his life for money.

In the same context, it is evident that darknet criminals have tendency to deceive each other. Such tendency could be exploited to motivate darknet criminals to return to the right path, by stating an excuse exempts or reduces punishment if one of them reports his partners in the crime, similar to what is stipulated in many types of crimes, such as terrorism crimes, bribery crimes, etc.

4 Procedural Issues

4.1 Investigation and Trial Procedures

Jurisdictions pay great attention to certain categories of society, whether they are victims or even perpetrators. This includes the Child Law of Egypt, that takes into account the psychology of justice-involved child (Hosny, 1998, pp. 876–877), hence, investigation and trial procedures are subject to different rules other than that for adults.

For example, the law specifies certain prosecution department for juvenile affairs, the juvenile prosecution addressed in Article 120 of the Child Law. During investigation process, preventive detention shall not be imposed on a child who has not exceeded 15 years of age at the time of committing the crime (Abdeltawab, 1997, p. 188). However, Marcus and Wilson (2016) state that certain jurisdictions may allow preventive detention for dangerous juvenile offenders. (pp. 108–109). Rather, in accordance with Article 119 of the Child Law, the Public Prosecution may issue an order for justice-involved child to be placed in a supervisory premise, or delivery to parents or guardian (Elshawarby, 1991, p. 85).

At the trial stage, and according to Article 127, the social observers have to create a file for each accused child that includes a complete examinations reports of physical, social, educational, psychological, and mental status of the child. A court has to review the file and examination reports before taking any action regarding the case (Elshawarby, 1991, p. 86).

Furthermore, and in accordance with Article 128, the court might issue an order for further and advanced physical, psychological, and mental examinations if needed. In such case, the court may place the child in a supervisory premise for certain period of time. The case shall be suspended until these examinations been completed.

These rules are stated to study the psychology of accused child, and factors and circumstances of the crime he committed, for rehabilitation and individualization purposes (Hosny, 1998, p. 937).

Article 125 of the Child Law states that the child has the right to legal assistance. In cases of felonies and misdemeanors punishable by imprisonment, accused child must be represented by an advocate during investigation and trial stages. Public Prosecution or court has to appoint an advocate for such purpose if the child did not so (Elshawarby, 1991, p. 85).

In the same context, confidentiality is imposed in juveniles courts, according to Article 126 of the Child Law, by limiting or prohibiting access of the public and media (Salama, 1992, p. 93), to shield juvenile offenders from social stigma, Cassation Court. Crim. No. 10812/67th judicial year 2005, (Bahnam, 1977, p. 147). That confidentiality is considered an exception to the general principle that requires criminal trials to be public (Hungerford-Welch, 2004, p. 68). The Egyptian law, as other jurisdictions, adopts the principle of publicity of criminal trials, Article 187 of the Constitution and Article 268 of the CPCE.

Moreover, Egyptian law provides protection for the identity of accused child. Article 116 of the Child Law punishes with a fine whoever discloses or reveals by any mean the identity of justice-involved child.

4.2 Personal Jurisdiction

International and regional agreements, as well as national laws, require special courts to try child offenders that are juvenile courts (Scheb & Scheb II, 2011, p. 39). Juvenile courts are regulated under the Child Law of Egypt, Articles 120–121. These courts are located in headquarters of governorates. The panel is formed of three judges, assisted by two experts, at least one of whom shall be a female, and the presence of the two experts in trial sessions shall be mandatory (Abdeltawab, 1997, p. 190).

The role of experts is not to participate in ruling process. Their task is to examine the case and all surrounding circumstances, to study social and psychological status of the accused child, and then to submit a report thereupon to the court. Experts' report is of advisory nature to the court (Hosny, 1998, p. 674).

According to Article 122 of the Child Law, a juvenile court has an exclusive jurisdiction over cases of accused and delinquency-exposed child (Abdeltawab, 1997, p. 196). However, if the child was over the age of 15 years at the time of committing crime, and an adult offender was engaged in the case, an adult court would have the jurisdiction to hear the case.

The reason of such principle is the presence of an indivisible link between the case filed against the accused child and that against the adult participant. That link requires, according to general rules, that both cases be filed before the same court (Hosny, 1998, p. 777).

Nevertheless, the adult court in such case is abide by rules and procedure stated for juvenile offenders, in particular, the court has to study status of the accused child, and may seek assistance of experts in such regard (Hosny, 1998, pp. 677 & 775).

It is to be mentioned that the Egyptian Public Prosecution referred the case to an adult criminal court and not to a juvenile one, in accordance with Article 122 of the Child Law, since the principal perpetrator of the crime is an adult.

4.3 Territorial Jurisdiction

Conflict of jurisdictions usually arises as a prominent issue in cases of cybercrimes, such conflict that might be exploited by cybercriminals to commit crimes and escape justice (Brown & Hermann, 2020, *pass.*).

In an attempt to address that matter, Article 15 of the UNTOC has identified the cases in which a state has jurisdiction over a transnational crime. Where jurisdiction is held for a state if the crime was committed in its territory, committed against one of the state's nationals, or committed by one of the state's nationals. Para 5 of the

article stipulates the necessity of coordination between engaged states to achieve jurisdiction and judicial competence. Moreover, involved states may establish a joint investigation authority, Article 19.

Article 16 sets out rules regarding extradition of offenders, requiring that the act constitutes a crime in both the state in whose territory the perpetrator is present, and the state requesting his extradition. The UNTOC requires that its provisions be the reference for bilateral treaties between states regarding the extradition of criminals. Para 8 of the article requires states to simplify and expedite extradition procedures.

Whereas the globalization of criminal activities—including transnational cybercrimes—has demonstrated the urgent need to achieve international cooperation in the field of crime control, investigation, inquiries, accusation, and prosecution (Chrysikos, 2018, pp. 191–192). Article 18 of the UNTOC stipulates that involved states should provide each other with the necessary legal assistance in relation to judicial procedures, prosecutions, and investigations.

Judicial procedures may include collecting evidence or statements and documents, implementing seizure, confiscation and inspection operations, examining and inspecting objects and locations, obtaining information, evidence and evaluations conducted by experts, obtaining original documents and relevant records, including government, banking, and financial records, identifying the proceeds of crimes, property, tools, or other objects or tracing them for the purposes of obtaining evidence, and other forms of assistance that do not conflict with national domestic laws.

Notably, in the case under study, these rules have been evident in the seizure of Kuwaiti mobile phones, computers, and SIM cards, their confiscation and delivery to the Egyptian authorities. The Egyptian authorities also have the right to know the perpetrator's income and property so that they can assess the situation and decide on the validity of the child's claims that this crime is not the first, and that all crimes he committed were paid for by broadcasting them on the darknet.

In the same context, and in accordance with para 13 of Article 18, involved state should assign a central authority to receive and direct requests for legal assistance, a role had been played by the International Cooperation Office of the Egyptian Public Prosecution.

On the other hand, court jurisdiction within Egypt is determined by the place in which the crime occurred, the accused person resides, or in which the accused person was arrested, Article 123 of the Child Law and Article 217 of the CPCE (Othman, 1991, p. 293; Shams Aldeen, 2005, p. 589).

That basic jurisdictional rule is applicable in comparative jurisdictions, such as in the UK, for example. Crime venue outlines court geographical jurisdiction. This is in application of the rule that each court has a specific geographical scope within which it exercises its jurisdiction (Ferdico et al., 2009, p. 55; Carmen & Hemmens, 2017, p. 10).

However, when the crime venue is determined outside the Egyptian territory, as the crime had been committed abroad, and the perpetrator does not have a place of residence in Egypt neither arrested there, a criminal action would be filed against him before the Criminal Court of Cairo, Article 219 of the CPCE (Surour, 1980, p. 299).

That rule applies to crimes committed outside Egypt, as the competent court cannot be determined based on the criteria of the place where the crime was committed, the accused's place of residence, or the place of arresting him.

5 Conclusion

This case has demonstrated beyond doubt dangerousness of the darknet and its impact on children. The question may arise about who was behind the inciting child, that is, who had incited him and created the idea of broadcasting such clips through the darknet.

The darknet has to be banned and the mere possession of tools to access therein has to be criminalized, even if actual access was not committed. The punishment could be harsher if the access was occurred. Additionally, the law may count using the darknet as a general aggravating circumstances for all crimes.

That issue also leads to another question regarding parents and guardians. As the child had have full chance and enough time to access the darknet and to plan for committing crimes. Presumed liability of parents or guardians could be established as a matter of law, as the case is an obvious indication of negligence in performing parents' duties toward supervising children.

The case also demonstrated the need for international cooperation in the field of darknet cybercrimes. Darknet cybercrimes are no less serious than organized crimes, even if they would be committed individually and unorganized. The UN may adopt a convention regarding the darknet and its impacts.

References

Abdelhamid Elshawarby (1991). Juveniles' Crimes. Dar El-Matboat Elgamya Pub. Egypt.
Abdelrahim Sedky (1986). The Brief in Egyptian Criminal Law. Dar El-Maaref Pub. Egypt.
Ahmed Fathy Surour (1980). The Intermediary in Criminal Procedure Law, Part II. Dar Alnahda Alarabia. Egypt.
Ahmed Fathy Surour (1981).The Intermediary in Criminal Law, Part I, General Part. Cairo University Press. Egypt.
Amal Othman (1991). Explanation of the Criminal Procedure Law. Egyptian General Book Organization. Egypt.
Ashraf Tawfik Shams Aldeen (2005). Explanation of the Criminal Procedure Law, fourth edn. October Engineering Press. Egypt.
Awad Mohamed Awad (1978). The Brief in Criminal Law: General Part, Part I. Dar El-Matboat Elgamya Pub. Egypt.
Catherine Elliott & Frances Quinn (2016). Criminal Law, 11th edn. Pearson Pub. UK.
Claudia Carr & Maureen Johnson (2013). Beginning Criminal Law. Routledge Pub. UK.
Diana S. Dolliver & Kevin Poorman (2018). Understanding Cybercrime. In: Philip Reichel & Ryan Randa. Transnational Crime and Global Security. Praeger Pub., USA.

Dimosthenis Chrysikos (2018). Fostering International Cooperation in Criminal Matters: The UNODC Mutual Legal Assistance Request Writer Tool. In: Philip Reichel & Ryan Randa. Transnational Crime and Global Security. Praeger Pub. USA.
George P. Fletcher (1998). Basic Concepts of Criminal Law. OUP. USA.
Hanna S. Kassab & Jonathan D. Rosen (2019). Illicit Markets, Organized Crime, and Global Security. Springer and Palgrave Macmillan Pub.
John M. Scheb & John M. Scheb II (2011). Criminal Law and Procedure, seventh edn. Wadsworth Cengage Learning Pub. USA.
John N. Ferdico et al. (2009). Criminal Procedure for the Criminal Justice Professional, tenth edn. Wadsworth, Cengage Learning Pub. Canada.
Joshua Dressler (2015). Criminal Law, third edn. West Academic Pub. USA.
Kent Roach et al. (2020). Criminal Law and Procedure: Cases and Materials, 12th edn. Emond Pub. Canada.
Mahmoud Naguib Hosny (1981). Explanation of the Criminal Law, Special Part. Rosalyousef Press. Egypt.
Mahmoud Naguib Hosny (1989). Explanation of the Criminal Law, General Part, sixth edn. Dar Alnahda Alarabia. Egypt.
Mahmoud Naguib Hosny (1998). Explanation of the Criminal Procedure Law, third edn. Dar Alnahda Alarabia Egypt.
Mamoon Salama (1992). Criminal Procedure in Egyptian Law, Part II. Dar Alnahda Alarabia. Egypt.
Mawad Abdeltawab (1997). The Reference in Explaining Juvenile Law, third edn. Dar El-Matboat Elgamya Pub. Egypt.
Michael Jefferson (2013). Criminal Law, 11th edn. Pearson Pub. UK.
Mohamed Eid Elgharib (1994). Explanation of the Criminal Law, General Part. Egypt.
Neikal Mahmoud Saloom (2009). Mutilation in *Sharia* and Law. Tikrit University Journal for Rights, Vol.1:4. Iraq.
Neil Boister (2016). The UN Convention against Transnational Organised Crime 2000. In: Pierre Hauck and Sven Peterke (2016). International Law and Transnational Organized Crime. OUP. UK.
Neil Boister (2022). An Introduction to Transnational Criminal Law. OUP.
Omar Elsaied Ramadan (1969). Explanation of the Criminal Law, Special Part. Dar Alnahda Alarabia. Egypt.
Paul Bergman (2020). Criminal Law: A Desk Reference, fifth edn. Nolo Pub. USA.
Paul Marcus & Melanie Wilson (2016). Criminal Procedure, 19th edn. West Academic Pub. USA.
Peter Hungerford-Welch (2004). Criminal Litigation and Sentencing, sixth edn. Cavendish Pub. UK.
Ramsis Bahnam (1977). Criminal Procedure: An Establishment and Analysis, Part I. Monshaat Almaaref. Egypt.
Richard Card (2012). Card, Cross and Jones, Criminal Law, 12th edn. OUP. UK.
Rolando V. del Carmen & Craig Hemmens (2017). Criminal Procedure: Law and Practice, tenth edn. Cengage Learning Pub. USA.
Sanford H. Kadish et al. (2022). Criminal Law and Its Processes: Cases and Materials, 11th edn. Aspen Pub. USA.
Stuart S. Brown & Margaret G. Hermann (2020). Transnational Crime and Black Spots: Rethinking Sovereignty and the Global Economy. Palgrave Macmillan Pub. USA.

Relevant Statutes of Egypt:

The Criminal Procedure Code, CPCE. Act No. 150 of 1950. Egyptian Gazette: Issue 90, Oct. 15th, 1950.
The Penal Code of Egypt, PCE. Act No. 58 of 1937. Egyptian Gazette, Issue 71, Aug. fifth, 1937.

Cybercrimes Law. Official Gazette of Egypt: Issue 32 bis (c), August 14th, 2018.
Child Laws. Official Gazette of Egypt: Issue 13 continued, Mar. 28th, 1996. Amended: Official Gazette of Egypt: Issue 24 bis, June 15th, 2008.
Anti-Human Trafficking, AHT Law. Official Gazette of Egypt: Issue 18 bis, May ninth, 2010.

Websites:

Alshorouk and Almasryalyoum newspapers (2024). https://www.almasryalyoum.com/news/details/3173058.
https://www.congress.gov/bill/118th-congress/senate-bill/1728.
https://www.shorouknews.com/news/view.aspx?cdate=26042024&id=188cf1ef-17d1-486f-b234-61310db86154.

Electronic Blackmail Methods against Children on the Dark Web and Their Psychological Impact



Noha Abd El Salam Abd El Tawab Soliman Kedwany

1 Introduction

Rapid and continuous technological developments and innovations have caused a major revolution in the world of communications. Although they benefit human life in many aspects of our lives, and have contributed positively to many fields such as the industrial, medical, educational and other diverse fields, it is a double-edged sword. Just as there are positives, there are negatives, and in a large and dangerous way. The morbid attachment to the Internet, social networking sites and electronic games that have come to dominate the minds of children and adolescents, who have become heavily dependent on the Internet, which poses a serious danger, especially with regard to the safety of children, among these dangers appears "electronic blackmail," which is considered one of the most dangerous cybercrimes targeting children and adolescents in particular, and this threat becomes more dangerous when it occurs on the "dark Internet," that dark area of the network that is difficult to access using traditional search engines, and is a safe haven for cybercriminals. The dark Internet is a part of the Internet that cannot be accessed using traditional search engines and requires special software such as Tor to browse safely and confidentially, as it is mostly used for illegal purposes, such as selling drugs, weapons, stolen data, human trafficking and other crimes, which poses a great danger about the "deep Internet," which represents approximately 95% of the Internet, as it includes all content not indexed by search engines, such as databases and corporate websites, but it is not necessarily illegal, unlike the surface Internet, which is the part that can be accessed via search engines Traditional search such as Google, including websites and public content, represents approximately 5% of the total Internet.

Electronic blackmail is one of the growing phenomena in the world of the Internet, especially in dark spaces that allow perpetrators to reach their victims in hidden ways

N. A. E. S. A. E. T. S. Kedwany (✉)
Waei Plus, Cairo, Egypt
e-mail: nohakedwany@yahoo.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_9

that no one can reach them. This dark environment attracts children and adolescents, who may be less aware of the potential risks. The methods of electronic blackmail against children vary through common methods such as sexual blackmail, luring through electronic games and temptations of money and gifts, phishing, and impersonation, as it can include threats to publish private information or sensitive images, which puts victims in a state of anxiety and fear.

Children are most vulnerable to these risks, due to their lack of experience in dealing with these situations, and therefore these children are exposed to significant psychological effects that affect their lives. The problem of electronic extortion is that children are exposed to severe psychological and physical pressure as a result of cybercriminals exploiting their photos or personal information illegally for the purpose of financial or sexual extortion. The dark internet is a fertile environment for such crimes, as it is difficult to track down perpetrators or prevent these illegal activities due to its anonymous and encrypted characteristics. In this context, this research comes to shed light on the problem of electronic extortion against children on the dark internet, and examines the methods of electronic extortion on the dark internet and the resulting psychological effects. By reviewing studies and research related to this topic, the research addresses the negative psychological impact on children exposed to this type of crime, such as anxiety, depression, and post-traumatic stress disorder, in addition to the social effects that may lead to social isolation or a decline in academic performance. The research also provides suggestions on how to prevent this phenomenon and protect children from the dangers of the dark internet.

2 Chapter One: Theoretical and Methodological Framework of the Study

Study Problem

Due to the successive and rapid developments in technology on the Internet and the increasing use of social media, which have greatly contributed to the circulation of personal data and information on the Internet and the invasion of individuals' privacy, which resulted in the emergence of new crimes unfamiliar to societies and called electronic crimes, which have diversified in many ways, including electronic blackmail, which is one of the greatest risks facing Internet users, especially children, because they are the most vulnerable to modern technology and the most targeted and threatened by criminals and cyberspace professionals, and from here the problem of the study was determined in identifying and analyzing the methods of electronic blackmail against children on the dark web and its psychological impact.

Importance of the Study

- Highlighting modern crimes resulting from technological development, and identifying their various methods and protection methods.
- The danger of this type of electronic crime and the resulting serious risks to children.

– Raising community awareness among parents to protect their children from electronic blackmail.

Objectives of the Study

– Shedding light on the use of the dark web and its risks.
– Identifying the methods of electronic blackmail that are used against children on the Internet.
– Analyzing the psychological impact that these crimes have on these children.
– Coming up with a set of proposals for ways to protect children from electronic blackmail.

Previous Studies

Previous studies are of great importance in determining the features of the study by reviewing the available previous scientific heritage. The study was divided into two axes:

The first axis: studies that dealt with electronic extortion.
The second axis: studies that dealt with the dark web.

2.1 The First Axis: Studies That Dealt with Electronic Extortion

The Analytical Study Conducted by "Abdul Manaf, Al-Jubouri" (2024**).** Through a discussion of the characteristics of cyber extortion, current concerns surrounding it, and pertinent national legislation and regulations governing it in Iraq, the US, and Malaysia, this study seeks to determine the efficacy of the cyber extortion law. To identify, investigate, and evaluate the problem from every perspective, analytical and descriptive methods were applied. Consequently, it was noted that Iraqi lawmakers did not truly want to enact a robust law that would combat cyber extortion, either by amending the Penal Code or by approving the Cybercrime Bill (2011). The primary part of the crime, according to an examination of its features, is extortion, which is combined with aspects of criminal intimidation intended to make the victim fearful and coerce them into submitting to the dishonest perpetrator's ill motive.

An Exploratory Study Conducted by "Youssef Daradkeh, Ahmed Abu Assad" (2023**).** The purpose of the study was to confirm how well upper primary school pupils responded to a preventive group counseling program designed to shield them against technological blackmail and gaming addiction. The assessment of cyberstalking and video game addiction was established, and a prophylactic counseling scheme was developed. There were 265 male and female students in the study sample. A sample of 24 students was chosen for the counseling program, and they

were split into two groups: the experimental group, which consisted of 12 students, and the control group, which had 12 students. The findings indicated that there was a moderate amount of exposure to online extortion and video game addiction. The outcomes showed that the experimental group members demonstrated a reduction in gaming addiction and an improved ability to cope with electronic blackmail compared to the control group. According to the report, pupils should receive preventive counseling through the current program before they are exposed to electronic blackmail or become dependent on video games.

A Survey Conducted by "AI-khaza, Ieh & Lahiani" (2023**).** The purpose of this study was to examine the connection between two cybercrimes—blackmail and harassment—as well as the effects they have on Jordanian society. Ninety public prosecutors employed by Jordanian courts were included in the study population. In the latter part of the 2020–21 academic year, the researchers employed the relational method. Public prosecutors in Jordan state that although cyberharassment is not very common, blackmail is. Additionally, a statistically significant correlation between blackmail offenses and harassment was demonstrated by the results among the sample members. This represents a statistically significant proportion. The study also demonstrated the six negative effects of harassment spreading: vilifying and threatening the victim; family and social disintegration; loss of morals; instilling uncertainty and low self-esteem; and unstable security. In order to fight cybercrime, the authors advise raising public awareness of the idea of electronic governance. Additionally, they advise governments to sign accords and pacts that make all forms of criminal activity illegal, pinpoint the locations of crimes as they occur, and specify the procedures for apprehending cybercriminals.

An Analytical Study Conducted by "Karrar Abed Ruwaida" (2024**).** which sheds light on railways, where we are witnessing an unwanted increase in their preparations, especially electronic extortion, which is due to reasons that may contribute to the implementation of these construction operations for everyone and unrestricted in terms of needs. And the use as well as applications and software that were used as a crime of electronic extortion, where the user used the descriptive analytical model in the completion of the research, with a statement of statistics in this nucleus of acceleration to show its importance in The research, has reached outstanding results that the crime of electronic extortion is the most important images of electronic imamate models widespread and influential in Iraqi society, that the material element in behavior and in electronic extortion is embodied in the Finenci, either the technical purposes carried out by the offender in order to obtain images or others, are infinite, they are multiple and owner, and also this crime is one of the intentional quantity that is sufficient for the existence of the general design in the concept of science and will.

An Analytical Study Conducted by "Omar Abdel Salam Hussein et al." (2022**).** It aims to highlight the primary issue when determining whether or not Iraqi law is sufficient to protect women from electronic threats, particularly in light of the fact that electronic blackmail against women is a malicious type of cybercrime that has proliferated in contemporary society and is a covert crime with significant social ramifications. Blackmail cases against women have generated attention on

social media during the Covid-19 pandemic, as a survey by the Iraqi Ministry of Interior for women revealed that 60% of women in the country had been victims of cyberblackmail crimes. The researchers employed the descriptive and analytical method to describe, analyze, and diagnose the issue in all respects, and as a result, the study improves the study clarified that the risks and consequences of electronic blackmail against women, especially in its extreme forms, can have dire consequences, such as placing victims under the control of the blackmailer. It also highlighted the importance of awareness in Iraqi society about the crime of blackmail to avoid women such a dangerous phenomenon. By providing a comprehensive discussion of a variety of topics and reasons that led to the expansion of electronic blackmail, the study also analyzed the most important aspects of litigation and community awareness regarding the crime of blackmail. Although the study only looked at cases in Iraq, its findings may nevertheless be useful to people all across the world.

2.2 The Second Axis:—Studies That Dealt with the Dark Web

An Analytical Study Conducted by "Li et al." (2021). Through a large-scale longitudinal measurement investigation on anonymous market listings and posts, the project seeks to identify the opioid supply chain in anonymous markets and forums. Overuse of opioids is a global public health issue impacting millions of people. In order to effectively address the opioid crisis and mitigate opioid consumption, it is imperative to get fresh insights into the opioid supply chain. In order to obtain data, a thorough crawl of anonymous internet marketplaces and forums was carried out. In order to find information pertinent to opioid trading activities, such as commodity, price, shipment details, and suppliers, the researchers then created a set of opioid-specific text mining techniques, such as opioid phrase identification and opioid trade information retrieval Subsequently, an extensive and extensive longitudinal investigation was carried out in order to clarify the nature of opioid trading in private marketplaces and discussion boards. We were able to identify 28,106 opioid product listings and 13,508 opioid-related promotional and review forum traces from 5147 unique opioid supplier identifiers and 2778 unique opioid buyer identifiers. These results offered insight into the opioid trade in anonymous marketplaces and forums and may prove to be an effective mitigation data point to shed light on the opioid supply chain. A total of 248,359 listings were collected from 10 anonymous online markets and 1,138,961 traces (i.e., chains of posts) from 6 underground forums.

The Analysis Study Conducted by "Bergman & Popov" (2023). Through a systematic literature review (SLR) that examines the presence and features of dark web crawlers, this study seeks to understand more about these topics. 34 articles were left after removing irrelevant ones from a selection of 58 peer-reviewed articles about crawling and the dark web. According to the literature research, the majority of dark web crawlers were written in Python and used the web scraping libraries Selenium or Scrapy. A Tor-based web crawling model was created and integrated into an already-existing software toolset intended for ACN-based investigations using

the information acquired from the systematic literature review Lastly, a series of experiments were used to evaluate the model's performance. The built crawler was successful in scraping web content from both black and clear web pages, as well as from dark markets on the Tor network, according to the results. This research adds fresh understanding about ACN-based web crawlers to the scientific community. In addition, it offers a model for digital investigations aimed at crawling and scraping both clear and dark web domains. The practical ramifications for retrieving and archiving content from the dark web are discussed in the conclusions, along with ideas for future research projects and leads for investigations.

The Confirmed Study Conducted by "Sönmez & Codal" (2021). Given that crime, terrorism, and other illegal activities are becoming more common in cyberspace, and that crime in the dark web is one of the biggest problems facing governments worldwide, this study aims to critically analyze the literature and highlight the research efforts in dark web studies related to terrorism. The dark web makes it difficult to identify criminals and track their activities because it offers anonymity thanks to special tools like TOR. Therefore, it has evolved into a platform that contains various criminal operations such as pornography, arms trafficking, drug trafficking, fraudulent documents, etc. The results of the study, particularly with regard to terrorism as it pertains to this paper, indicate that there is a deficiency in the body of literature regarding scientific studies on terrorist activities. To address this gap, a variety of scientific methods should be employed to detect and combat terrorism on the dark web, including advanced artificial intelligence, machine learning-based image processing and classification, natural language processing techniques, hash value analysis, and sock puppet techniques.

An Analytical Study Conducted by "Ovosuri, Hendrady" (2023). The goal of the study was to determine how the Dark Web affects society by methodically examining pertinent books and scholarly publications to learn more about the Dark Web's operation and social effects. According to the study's findings, the Dark Web helps to facilitate a lot of cybercrimes. Despite the fact that governments and regulatory bodies have offered strategic detection approaches on the Dark Web, fraudsters have learned to adapt to these strategies and frequently find ways to evade detection measures over time. The research suggests that for efficient monitoring, regulatory bodies and cyber threat intelligence should routinely assess detection methods Criminals should also take additional cybersecurity training to make sure they are up to date on the most recent scientific findings about the safe management of the Dark Web. Further study is also required to concentrate on raising public knowledge of the risks associated with the Dark Web.

Study Questions

- What are the methods of electronic blackmail used on the dark web against children?
- What are the psychological effects on children's health resulting from these crimes?

– What are the methods of protection to reduce electronic blackmail against children?

3 Chapter Two: Cognitive Foundation of the Study

It is divided into two sections:

The first section—deals with electronic blackmail methods against children.
The second section—deals with the dark web.

3.1 The First Section: Methods of Electronic Blackmail Against Children

Definition of electronic blackmail.

Methods and forms of electronic blackmail against children.

Examples of cases of electronic blackmail.

Definition of Electronic Blackmail
Electronic blackmail is a criminal conduct that exploits victims for unlawful gain. It frequently uses sensitive material, particularly opposing perspectives, to compel victims into cooperation. This pressure takes away their free will as they try to prevent defamation or controversy, emphasizing the need for punitive actions against such exploitation (Maarouf, 2023, p. 2003).

Electronic blackmail is the act of abusing another party for material or emotional benefit by threatening them with sensitive digital records such as images, videos, or papers. These materials are frequently obtained illegally via hacking, email, group chats, or messaging apps. The blackmailer utilizes this content to pressure the victim, either for financial or moral gain, or to destroy their reputation or well-being (Makkawi, 2022).

Electronic blackmail against a child is any illegal act or word, written or worded, addressed to a person toward an 18-year-old child. It involves a harmful act committed through the use of communication devices consisting of a mixture of fear and terror intended to force him to do something specific (Quraina, Rasheed, 2011).

Methods and Forms of Electronic Blackmail Against Children
In the coming years, I have sponsored the participation of electronic blackmail against children, because the category of children does not have sufficient experience in dealing with technological means in all its forms, and it is looking forward to what is new without knowing the results, which easily exposes them to exploitation by others, And also the lack of difference from the family to learn the children's chat and the definition of the Internet, and also the disintegration of the family, and the Brazilian

vacuum and the worker from their children, or think about gender discrimination cruelty that leads to the main mutual trust between parents and children, which makes them resort to strangers in the virtual world, and also display the details of personal life on social networking sites, which makes snoopers and stalkers of cybercriminals recognize them from children with ease (Abdel Aty, Minshawi, 2021, 137).

Stages of Electronic Extortion

Electronic blackmail is achieved by analyzing the details through several stages, starting from the request, then resistance, then submission and repetition, where the first stage begins that the blackmailer performs the process of searching for the victim through the person's study of him, and follow-up publications, pictures and his psychological state and knowing the nature of his social life, and whether he has psychological pressure or family problems, then the second stage comes with his arrival On information and privacy data admired by the victim, by sending a friend request from the blackmailer to the victim, and then the conversations begin to be sacrificed and contain scandalous, whether by text, sound, image, sound and image together, or by penetrating the target device or stealing its data and content, then the method of blackmail and threats begins, monitoring the information that J does not want to know her distinct, and the blackmailer continues to bargain financially or practice an indecent act and does not press the button J for the blackmailer's requests comes the stage of defamation and drunk e special on social media platforms or YouTube, whether on the hacked registration page or on the page of the offender or in the name of Mstaa, and the problem increases In the case of fabrication of images, videos and audio through advanced techniques such as deepfakes, thanks to the distortion of the blackmailer's submission, his requests are repeated with more material or sexual blackmail (Yassin, 2024, pp. 174–175).

Electronic Blackmail Techniques Against Children

There are many methods and patterns that Al-Majeed resorts to in electronic space to exploit children to blackmail them, and one of these methods sends the blackmailer a message to everyone the goal or help as follows:

—Hello.

—You're welcome … Who is it?!

—I know everything about you and what you do in secret from your family, and you are videos of you, click on this link and see.

This is how the dialogue begins on how to identify electronic extortion, and three again and differently, where this blackmailing fraudster is not really required to have information about NBC, we want to use a method that suggests his knowledge and his personal tasks and private secrets, only at the push of a button of control. The frightened link that accompanies him as much as possible with the great news allows him to hack corporate accounts on social media, as well as access the contents of his phones, and desirable people (Al-Tahhan, 2024).

Non-Grooming

Most modern games try to achieve players' interaction with rewards and loots such as in-game, spells, upgrades and weapons that are found during gameplay and progress

in the game, and allow many games also to work within the game, which you can participate in or win through mods, and these rewards can be converted into money True, and since coins and bonuses are highly valued by players and difficult to obtain, and offenders have offered them in exchange for social and emotional interaction, grooming is the creativity of colleagues and the formation of relationships with children with the intention of isolating them sexually, and this can happen directly or online, and it has been realized that between 1% and 20% of children who use the Internet face requests to share sexual content, sexual revolutionary development, or share their photos without consent, or face blackmail. Online, while most of these things happen on social media, I have also started playing games in the wake of children and blackmailing them (Kavenagh, 2023).

Children also face many forms of abuse and exploitation in various forms via the Internet, including:

Cyberbullying: Through fame or social exclusion and emotional harassment.
Sexual Representative: Distribution of explicit and violent sexual content and sexual harassment through cyberspace.
Sexual Exploitation: Through production the new element in Christianity is pedophilia.
Cyber Extremism: Through ideological inoculation, recruitment, and threats of extreme violence.
Experimental Registrar: Through identity theft, phishing, hacking and fraud.
Healthy Habits: Internet inducements for illegal behaviors such as cheating, plagiarism, gambling, drug trafficking and sexual messages (Kumar, 2021, pp. 1325–1326).

Examples of Cases of Electronic Blackmail

Of the children and teenagers who have seen the blackmail, it has been mentioned by the models of the Childline website, which is a free service for children since the age of 19 in England for those who need support or participation, as we are increasing number of calls from children and adolescents who are exposed to Malaysian youth blackmail on the Internet, and then these cases.

She contacted a 17-year-old girl, who was 17, a "girl" on social media to recognize her at his age, and after accepting the messages, she sent her a front photo. Then she started blackmailing.

The 16-year-old, a child victim of sexual blackmail, was identified online and sent his nude photo, and was distinguished from they would share the photo if he sent them money, and he did not know them in real life.

Shaker said they were contacted on Instagram, Snapchat and Wizz, in some cases they are asked to go to a private messaging app where communications become private before being asked to view photos or short videos, young girls who are 16 years old and semi-naked are introduced on a private messaging platform and then take over It's his turn to give back, send from the nudes and then immediately ask him for £100 otherwise you'll send two copies to his followers.

Since then, I have started generating sophisticated AI images on a large scale, usually from cases of extortion where it is done by generating fake inappropriate images of children and threatening them if they spy on money or spy other nude photos, I will share them with people.

In one case, a 15-year-old girl stood out, with whom she stood in solidarity huge, and used "really compelling" beautiful photos of her face and her sleep ice, after she was apparently taken over from her Instagram accounts, and this person has long benefited from massive fake-up with artificial intelligence. Something made a video on her face and thinks that it is for money, and if she does not pay, she will end up alive Guardian, (2024).

3.2 Section Two: The Dark Internet

Definition of the dark web.

The dark web's appearance.

Legal and illegal uses of the dark web.

Dark web dangers.

Electronic blackmail techniques against children on the dark web.

Psychological effects on children from electronic blackmail on the dark web.

Ways to protect children from electronic blackmail on the dark web.

Definition of the Dark Web

Most internet users believe that the dark web is solely used for criminal activity, which is partially correct. However, understanding the dark web necessitates a grasp of the internet's overall structure. The internet is made up of a linked network of servers, computers, and other devices, and it is divided into two parts: the surface and deep web.

The surface web includes sites that are easily accessible using standard browsers and search engines such as Google, Yahoo, and Bing, although it only covers a small portion of the internet. The deep web, on the other hand, contains content that cannot be accessed using ordinary browsers and accounts for around 90% of internet traffic. It is thought to be between 4000 and 5000 times larger than the surface web.

The deep web contains data from social networking sites like Facebook, Twitter, and Snapchat that can only be accessed via APIs, as well as file sharing services like Dropbox and Google Drive and instant messaging data.

On the other hand, the dark web makes up less than 0.01% of all websites on the internet and is a very small and challenging to reach portion of the deep web. There are hundreds of millions of conventional websites and roughly 45,000 dark web domains. Use a specialized browser like The Onion Router, or Tor, to access the

black web. Since the password to the dark web is typically anonymous, it is a haven for crooks and political dissidents (Chertoff, 2017).

The term "dark web" refers to websites that are hidden behind several layers of encryption and are inaccessible through conventional web browsers or search engines (Egan, 2019).

The term "dark web," "hidden web," or "hidden internet" refers to a collection of websites that conceal their IP address using anonymization tools, the most well-known of which are Tor or P2I. This means that websites on the dark web or hidden web cannot be securely accessed through these tools because they are not listed on common search engines like Google. Additionally, hidden services have a unified source address URL that ends in "onion," which is a routing technology that enables anonymous communication over computer networks (Gehl, 2014).



The Dark Web's Appearance

In 1960, the concept of ARPANET—a computer communications system that enabled device-to-device communication—was born. The military, which was waging the Cold War at the time, quickly adopted its use after it was invented by academics. The U.S. Department of Defense's Advanced Research Projects Agency (ARPA) aimed to create a computer-based communications system without a central core. As a result, ARPA started sponsoring ARPANET with the intention of using it to link computers at research institutes financed by the Pentagon over phone lines. Despite the government's privatization of ARPANET, researchers were still able to experiment greatly and use it to facilitate the first illicit internet transaction. Students at Stanford University engaged in a marijuana trade with their MIT colleagues in the early 1970s using ARPANET accounts at the Stanford Artificial Intelligence Laboratory. This led ARPANET's creators to divide the network into two sections, MILNET, in 1983 so that military agencies could use it. The foundation for the Internet was created by the military and a civilian counterpart of ARPANET. When the globe was first exposed to the Internet in 1983, all of the data was kept there

in “data havens,” which functioned similarly to tax havens but allowed mountains of data to be exported to nations with liberal legal restrictions, keeping it out of the hands of domestic governments. Public access to the Internet began in August 1991. Online, more illicit transactions started to take place, this marked the beginning of music consumption and the development of MP3 compression formats, enabling CD ripping without authorization. Before shortly, illegally ripped music started appearing in forums and on the internet. Additionally, Tor, a private Internet surfing network that would subsequently play a significant role in providing access to the dark web, was still in its early phases of development during the 1990s (Kastner, 2020).

The most popular anonymous network is called Tor. Originally from the United States, it was released as The Onion Routing in 2002. The term Tor refers to both the software you install on your computer to run Tor and the network of computers that manages Tor users’ connections to websites through a series of virtual tunnels rather than a direct connection, allowing both organizations and businesses to communicate with each other. Individuals can also use it to share data across public networks without jeopardizing their privacy. They use the computers of other users to reroute their Internet data, making it impossible to identify the originating user. Tor builds strata (much like the layers of an onion) and conceals users’ identities by routing traffic through those layers. Information is encrypted as it travels across Tor’s network of “relays” on computers all over the world to move between different layers. All traffic over Tor passes through at least three relays before reaching its destination. The “exit relay” is the final relay. The source of the traffic over Tor is identified as this relay’s IP address. Users’ IP addresses are disguised when using Tor, so when they connect to any website, it seems as though they are coming from a Tor exit relay IP address, which might be located anywhere in the globe (Finklea, 2015).

Since the introduction of private surfing networks like Tor, Biometric trends started with websites that groups of people followed, and then a community of people followed them, there are generally trends targeting a large number of sites, and therefore they were added illegally, resulting in the emergence of cryptocurrency that was p. It was founded in 2009, called Bitcoin, and it is one of the first digital currencies to facilitate transactions unknowingly, and in 2010 after the issue of anonymous transactions and illicit sales on the dark web was resolved, It enabled users and activists who required it during this period to access the Tor Browser version, particularly during the Arab Spring., and not only Tor Not only did people have online identities, but they were also allowed access to resources for the success of social media and blocked sites, Moreover, in 2011, Gawker published a presentation of the Silk Road, a dark web marketplace “This exhibition helped direct the process of making the purchase and sale of illegal drugs as simple as purchasing used electronics.” the ban movement directly to Silk Road, which quickly boosted its sales. Tax Office. The campaign to shut it down began, and it was swallowed up in 2013 as the Silk Road attracted nearly a million users in a short time, making women around the world take action against the Internet (Kastner, 2020).

Legal and Illegal Uses of the Dark Web

Legal Uses of the Dark Web

Although using the dark web might initially appear to be notorious, it has some resorts that it considers important It's legitimate for Tor and anonymous browsing, for example, in epidemiology that may use government confrontation to spy on and suppress political opponents, often the internet is a place to avoid distancing and careful governments, Users should exercise caution when using dark email and closely monitor security, making sure to regularly update security software, use a VPN when browsing, and avoid using regular email addresses, even with this additional layer of protection.

Illegal Uses of the Dark Web

Some of the most prominent criminal and illegal activities that take place on the dark web include, for example, displaying data on bank accounts, credit cards, countries and hacked companies for sale, selling weapons illegally to individuals and unofficial entities, and trading in human organs. Some people also communicate with hackers on the dark web to hire criminals to take revenge on people by hacking their mobile phones and recording their calls in order to blackmail them for a fee, in addition to selling pornographic materials to people living in countries whose laws criminalize the publication of such materials. People also film pornographic films of themselves and publish them on this platform for huge sums of money, as well as hiring people to carry out terrorist acts, trading and selling cryptocurrencies "Bitcoin," the value of which is not subject to any central bank, and also practicing sadistic acts by broadcasting a game live on the dark web run by gangs that have kidnapped people, and holding an auction with huge sums of money amounting to thousands of dollars, for whoever pays the most to choose the way the kidnapped victim will die (Amankids).

Dark Web Dangers

Malware: It is formed from OP programs that infect devices with different techniques, such as clicking on malicious links, there is always a chance that you will click on a picture, link, or harmful content when you go dark programming since you won't know what is safe to click on. This may cause damage to the devices and if this spyware is installed on devices without the knowledge of their owners, enables it to spy by accessing the device's camera, and if keylogging software is installed on the device, Keystrokes and data, including credit card numbers and passwords, can be tracked by it.

Legal Consequences: A lot of illegal history happens on the dark web, and you can be considered complicit in this activity if you participate in parts of the dark web where cybercriminals are, for example, if you end up in a chat forum with illegal activity or carrying out inefficient purchases, you may face complications.

Financial Fraud: Going to the dark web can also put you at risk of being scammed financially. Black markets on the dark web take advantage of those who try to buy illegal items on the dark web by taking payments and then never providing the requested services.

Blackmail: Dark web visitors are vulnerable to blackmail by cybercriminals. If you visit the dark web without connecting to a virtual private network (VPN), cybercriminals can use this to their advantage to find out your identity by tracking your IP address. Once a cybercriminal knows your IP address, they can use it to find out where you live. If they find out where you live, they may try to blackmail you by saying they will scam you if you don't pay them—resulting in you losing money. Doxxing is a cyber threat where someone posts someone's personal information online without their permission.

Personal Information and Exposed Credentials: Dark web criminals use it to publish and sell personal information they have stolen or collected from public data breaches. If your personally identifiable information (PII) ends up on the dark web, your identity is likely stolen, which is mentally and financially difficult to recover. Posting your PII on the dark web also makes you vulnerable to targeted cyber-attacks that are difficult to detect since they are tailored to you only (Trevino, 2023).

Electronic Blackmail Techniques Against Children on the Dark Web

There are many methods of organized criminal gangs on the Internet who exploit children in their criminal operations on the dark web, which are considered one of the most dangerous cybercrimes, as these criminals rely on multiple methods to trap and exploit children due to their young age and lack of sufficient awareness of technology and its dangers. Common methods include sexual extortion, luring through electronic games and the temptations of money and gifts, phishing, and identity theft. The following is a review of some of the methods:

Sexual Blackmail

Sextortion is one of the most common forms of cybercrime against children, where a criminal persuades a child to share sexually explicit images or videos, then threatens to publish the material if they do not comply with their demands, which may include sending more images or money. An analysis published in the Internet Watch Foundation's (IWF) annual report found that 2401 so-called "self-generated" images of children aged three to six were found on the open internet in 2023. "Self-generated" images are where a child is persuaded, coerced or tricked by the blackmailer into performing acts via a webcam or handheld device. Nearly one in seven were Category A images—the rating it gives to those that show the most serious abuse. Six in 10 showed "sexually explicit nudity." Analysts who reviewed some of the images found that many were "taken at home in children's bedrooms or in family bathrooms when the child was alone or with another child such as a sibling or friend." Sometimes the children were completely unaware that they were being recorded, and that someone else was They are being warned that children aged three to six are sexually naive and will not usually be aware of the potential for this type of sexual behavior, and

the report also suggests that online child abuse material is becoming more "extreme" with the charity reporting a 22% increase in Category A images (Vallance, 2024).

There is undeniable evidence that the Internet has led to an unprecedented increase in the development of child pornography. One contributing factor has been the significant reduction in barriers to entry due to advances in technology. The increased accessibility and ease of use of advanced editing software and cameras have simplified the creation and distribution of child pornography. The term "child pornography" is explicitly defined under the Protection of Children from Sexual Offences Act. According to the section of the law, child pornography is described as a visual display that depicts explicit sexual activity involving a child.

Solicitation Through Electronic Games and the Temptations of Money and Gifts

E-commerce is currently no longer just entertainment or entertainment for children and adolescents, but has become many games, many of which are shared by voice and text chat that encourages children to chat with strangers and much more for supervision, where they are allowed to enter into inappropriate conversations or are allowed to share personal information and can be used for blackmail, where users can hide their identity behind the avatar, allowing criminals to demonstrate to cover between 10 and 15 years, which is Opportunities for international cooperation actors to use Liechtenstein computer users and other diversity to gain water through targeted fishing and cyber goals of social engineering, and then to become children and adolescents who have managed to acquire cybersecurity knowledge one major chooses to choose from.

Kaspersky experts have presented a report about starting with all the young children and toddlers in the worlds of special games about the most popular children's games, which have an average age of the player between sixty-six years and which allows users to play online in a virtual world with friends and unfashionable users, from January 2022 to December 2022, and I have selected the game to the top 13 games, series and platforms to download, in addition to evaluating direct hunting activities, and discovered many reasons that led to the damage of players, and the main result was led by more than 232,000 users who came across around 40,000 dangerous spreads in 2022 while playing well-known kid's games; Kaspersky's security solutions discovered more than seven million attacks in 2022 related to well-known kid's games, leading to an increase to 57 percent compared to 2021, and what Internet users exploit the most is Minecraft and Roblox, in 2021 and 2022, the best children's games have differed in terms of the number of users who have been attacked Poppy Playtime and Toca Life World, mainly for children aged 3–8 years, which tends to be that cybercriminals are trying to resist even the youngest players, most likely, to gain access to their parents' devices, as Kaspersky experts have noticed a 41 percent increase in the number of influential Around 10,000 players in 2022 were attacked by people downloading malware files purported to be Brawl Stars, according to Kaspersky data, hardcore games targeted by cybercriminals mostly targeted Roblox, Minecraft, Fortnite and Apex Legends. In the collection, more than 878,000 phishing pages of these four games were created in 2022. Of these, 823,000 were created for

Roblox solo. In January 2023, the number of Czech cities reached a record 132,794 Czech fishing sites related to Roblox, when they were set up in 2022 (123,832) (Kaspersky).

Perpetrators of the sexual contribution have found ways to take advantage of technology for children, manipulate and exploit them, online, it has helped them use multiple platforms and games to evade a lot of control measures, the changing nature of the games and the wealth of communication that players use make this space very difficult to moderate, organize and organize, in addition to that it assumes its behavior multiple platforms, and experiments Most modern games keep players engaged with bonuses and "loot" such as in-game handling, spells with, upgrades, weapons that can be found during gameplay and progress in the game Many games also allow in-game action, which can be shared or earned through a maker, these rewards can be converted into real rewards, since creative workers and rewards are highly valued by players and difficult to obtain. Heaven was presented in exchange for sexual and pictorial interaction (Kavenagh, 2023).

Phishing: It consists of online identity data and seeks to misappropriation of information such as online service passwords and credit card traffic information from people (Alkhalil & et al. 2021).

Fraudulent attacks typically last longer than four months, and although victims may be identified as children, they frequently succeed in causing financial harm to the victim and completing personal business. As a result, according to 2017 research, over a million kids in the US alone found their identity, costing the country $2.6 billion. When someone is properly targeted because of their status, it is usually easy to identify them. In certain instances, children's desired identities are larger due to their current credit profile (Carle & Ophoff, 2024).

Data from the Internet Crime Center indicates that extortion, online shopping scams, and phony scholarships and contests are just a few of the scams that target minors. These crimes have the potential to result in identity theft, financial loss, and emotional pain. Phishing, for instance, is a prevalent kind of child pornography.

Online Shopping: Youngsters or children may begin to receive advertisements or messages that offer discounted goods, like a $25 iPad. If they provide payment details, they may not receive the removed item and their money will not be deducted, but thieves may steal their payment details and other personal information.

fake Competition: Youngsters could be persuaded to enter a fake competition that costs money, or they might be offered the chance to win and then requested to give personal information or make a payment to claim a prize that never materializes.

Phishing Scripts: Fake text messages that appear to be from reputable websites or accounts, such as social media or gaming sites, might come across as urgent and demanding. Typically, these messages ask kids to confirm their passwords, user information, or credit card numbers, or they may contain links that download spyware directly to their phones.

Sexual Fraud: Blackmailers compel youngsters to post graphic pictures or videos of themselves online. Usually, they pose as someone their own age who is looking for a relationship or offers something for free in exchange. The fraudster may then say that he already has an incriminating photo or video, or he may share without the victim's knowledge, and threaten to post the images online unless the money is paid.

Online Gaming: Children may be coerced into disclosing private information like names, addresses, and account passwords when they make online friends. Free in-game money, "skins," or other enticing bonuses might entice kids to click on websites that download spyware or malware or divulge credit card information.

Online Quizzes: By asking for details like birthdays, pet names, street names, favorite TV shows, or best friends, it is possible to conduct an apparently risky review of children's personal recommendation data. We frequently use this information as word passages or snapping for security questions, which allows access to the children's accounts.

Talent Exploration: Along with the child's cash resources, scammers may obtain the child's personal information or end up with photographs or video footage through an alluring message or commercial. The youngster may pay the subscription cost for phony talent competitions to participate or make a choice.

Celebrity Attractions: Little ones could not comprehend that by clicking on a pop-up window might lead to problems. Clicking on a link l could lead to downloading useful programs or spyware to your gadget or PC, and cutting money and personal business clicks such as number credit cards or passwords.

Money Transfer: Does your adolescent or child have a cash app on their phone, such as Venmo? Caretakers Transfer money to users; send a text message stating your goals, reply, and request that the recipient transfer it back. Only when your child has sent the payment realizes that the original payment did not benefit.

Financial Aid Scams: By paying an application fee up front, scammers might entice teenagers to apply for fictitious grants, scholarships, or financial aid for college. They may suggest the adolescent has won a financial reward but must pay to claim it. In order to confirm their eligibility, some con artists request bank or credit card details before removing funds from the account. Alternately, they can request the password and information from a student's Free Application for Federal Student Aid (FAFSA), which would allow them access to private financial information (Axelton, 2022).

3.3 To Safeguard Personal Data and Information from Phishing Attacks, Should Take the Following Steps

Rely on Password Managers

Password managers offer a secure way to generate and manage strong, random passwords. They also issue alerts when attempting to use passwords on phishing sites, preventing login information from being entered if the site is not trusted. This reduces the risk of assaults aimed at stealing credentials.

Avoid Dealing with Untrustworthy Links and Attachments
You should avoid clicking on links or opening attachments sent by email or text message from unknown sources. Hovering over suspicious links to see the true destination or utilizing specialized tools such as Google's Transparency Report to evaluate their security can reveal the truth.

Use Email Scanning Tools
Email scanners enable the proactive detection of malware-containing attachments. Investing in these solutions increases protection against email-based phishing assaults, lowering the risk of sensitive data leaks (Keeper 2024).

Identity Theft
Birth babies did not survive the electronic they have become a commodity that is advertised for sale on the dark web, where the data sold includes names, phone numbers, addresses and social security numbers, the children are immune to identity theft, where a hadith analyzes the broker's data in many markets, and advertises stolen personal information, and transparently relates to children, and then examines the data that comes from hospitals and pediatricians, and contributes to the broker's achievement in Dream's marketing indicators. and empire. Emily Wilson, vice president of research at cyber company Terbium Labs, alerted the motherboard for the first time to data lists, in order to be the dream of the largest online dark web market at the moment, for very young children, in order for criminals' data to be obtained through access to networks or government accounts, where the broker markets as a complete set of "fullz" Any information about someone's identity, or at least a simple task including to commit the form of permissible orientation, the researcher says that the child's data includes name, address, phone number, data maps and social insurance number (many scientists apply for their newborn children's social security numbers, which belong to the federal government). Each set of data costs $10 each or $790 for 250 volts, or $490 for 250, depending on the market the fraudster might buy from, and one data tracking list says on people born between 2000 and 2010, meaning children between the ages of 8 and 18, fraudulent investors from this data, most of them will open economic lines to serve another five years and this is plenty of time to create some moneymakers. "Celebrities" and it is also famous that the publisher posts in the advertisement that these children "generally come from good families who can provide [and pay for] medical support" (Sjouwerman, 2018).



Product description

NEW STOCK DECEMBER 2018

-This listing is KIDS SSNDOB info from pediatrician and other medical databases.
-Years 2000-2010. Bulk discounts available
-The source indicates that generally speaking the kids come from good families that can provide and pay for medical support.
-Very cheap and very fresh. No reselling

You will receive the following data, format may vary for different sources but this will always be there:
Name I Address I Phone I SSN I DOB

3.4 Psychological Effects on Children From Electronic Blackmail on the Dark Web

Rajaa Al-Ajmi As a result of the psychological treatment at the Child Protection Center, electronic blackmail is a deviant and non-agreed, social and legal control, and this deviation in the virtual content is only a translation and reflection of the realistic behavioral style The blackmailer himself and a way of life that he employed through cyberspace, exploiting private people, including children, for purposes in himself, and as a result, children were infected with psychological electronic blackmail on children, which led to the burning of adolescents and suicide The psychosocial effects that children are exposed to due to electronic blackmail, which appears through and because the child's comprehensive health status is always growing, such as introversion, removal from children, unjustified fear, exaggeration of negative feeling, social withdrawal and reluctance to deal with others, and he feels confident in himself and in these events, where electronic blackmail leads to self-flagellation and tension always, which makes him in doubt and insecurity of his social environment It can also cause electronic blackmail in cases of simple depression in the child, which may develop

into severe depression as a result of a contract situation and decades that he is going through, and this affects the child's ability to coexist normally and leads to sleep problems, which may require the effect of drug treatment and the child is exposed to psychological burnout or band resulting from the nervous and psychological effort of the responsible in thinking and psychological pressure that he is exposed to for not disclosing to those close to him and bearing secrecy for a long time, and He even attempts suicide after we saw the child depressed or exposed to psychological pressure from great fear and fear of revealing the matter or fear of the family combined resort to them to self-harm and attempt suicide, as well as optional silence or what is called in psychology selective mutism, a condition that some children, especially those who reach between 7 and 10 years, are exposed to as a result of psychological trauma and severe fear of the reactions of the people who abuse them or the aggressor or blackmailer himself In this case, the child resorts to silence and refusal to speak and the linguistic interaction of the driver, and may also induce post-traumatic stress disorder, especially if the child is subjected to sexual blackmail, which causes him multiple and complex origins such as sleep disorder, language disorder, anxiety disorder with guilt and remorse, and possible social effects Family disintegration as a result of the problems that may result from holding each party responsible for the educational situation of others, in addition to its connection with the child can lead to the reinforcement of Social relations within the family, and these effects have not been addressed, psychological treatment must be provided to children of all kinds, whether individual or collective, in addition to providing psychological and social support to children, so I skipped the digital login that passes through it, and the child must be educated about how to use the digital sports Internet safely and physically and psychologically (Al-Ajmi, 2024).

Electronic blackmail affects the lives of children significantly, so children must be observed and the signs that appear on their screens for electronic blackmail, most notably: increased attention, fear and use, only simple isolation, spending less time in the company of family and friends, changing sleep habits of events and as a result of damage control, the charm of the joy of feeling of loving realistic pleasure, unusual work time difference, spending more time using everyday electronic devices and ensuring constant connection to the Internet, aggressiveness, The course of educational level and academic achievement, a noticeable change in the habits and times of frequenting the toilet.

Naturally the age of the Internet Dark for teens and teenagers Who are curious rebellion or a sense of immunity where This hidden part of the internet can be a magnet for a young man who is fascinated by the forbidden or people who study in societies who seem to understand them better than their real counterparts in the world, However, that curiosity leads them to the darkest and because the break on the web, where the scope of illegality, disturbing content and dangerous ideologies expands, and a lot What the dark web application does not start in its content but in the promise of exploring something "forbidden," which can be particularly tempting and teens who navigate children in their identity and independence and Would be This curiosity or exploration is the result of Injury Psychological On children where This can lead to exposure to harmful content such as violence, pictorial, use or extreme

thoughts of anxiety, depression, post-traumatic stress and a distorted view of reality, Dealing with communities that glorify harmful behaviors can lead to an increase in serious, such as violence or abuse narcotics and normalization as an acceptable adaptation mechanism (Samurai Security, 2024).

Protection Methods

The history of coverage must be developed and updated, digital electronic awareness of risks, games and chatting become the most dangerous in terms of communication with strangers and their dispersing effects and potential health risks (Abu Amsha, 2024).

Educate children about not sharing personal information or photos online with unknown people, using antivirus software, device firewalls, and children's online activities appropriately.

The driver uses the Internet through navigation to get time for the school work screen, and time times are available for entertaining educational programs for children, such as open sites for parks or museums or communicating with classmates to activate online learning, and children can spend their time on the web as stated in the activities and learn about cooperation and kindness, A number of educational platforms and technologies have been created that provide parents and teachers with a large range that must be supported by increasing need and familiarity with technology, in this new social context, pediatricians can practice the practice of advising families on the best way to create their children's time and those who use it. The number of unstructured people is growing online (Ferrara et al., 2021).

Children must be trained on how to recognize sorcery hunting, which you can guide them on what to do if they encounter it for beginners, definition of never specifying anything without a guardian, the same applies to clicking on any links in emails, direct messages or celebrity windows, if they see a phishing scam, and they should tell the B or anyone afterward more confidently immediately, if they do not Parents or anyone have enough to make sure they want, so, if there is no other action, Train them on how to quit running any apps to use and their devices in case etc. Avoid children writing down any personal information without a hit, this can show up when you create an account for a game or online community, let your children know the exact time they are asked for personal information and always check who wants to get permission to get permission (Get Cyber Safe, 2022).

Study Results

The results showed the multiple methods of exploiting children by criminals on the dark web, due to their young age and lack of sufficient awareness of technology and its dangers, which makes children prey to electronic blackmail, through luring through electronic games and the temptations of money, gifts, and phishing to blackmail them sexually or financially with successive threats.

The results also showed that perpetrators of sexual crimes exploit gaming platforms to attract children through them, as most modern games try to maintain player interaction by completing certain tasks through which rewards and gifts are obtained, such as in-game currency, spells, equipment, upgrades and weapons that are found

during play, which players can buy or earn by completing tasks. These rewards can be converted into real money, which is difficult to obtain, as perpetrators may offer them in exchange for sexual interaction or for sending them inappropriate pictures.

Criminals also use fake text messages that appear as gaming sites or social networking sites, which children are easily deceived by, through phishing, which is one of the most common threats to users, especially children, which aims to steal the identity and financial damage to the victim, and to access their personal accounts and the accounts of their parents. The results also showed that children are exposed to serious psychological and social effects due to electronic blackmail that may lead to suicide, which appears in behavioral forms such as withdrawal and isolation from those around them, unjustified fear and hesitation in the simplest situations, and loss of confidence in oneself and in those around them.

Recommendations

- Technology companies and electronic platforms must work to create solutions that help protect and secure children from such crimes that take place on the dark web, electronic blackmail, and all forms of electronic violence that children are exposed to, and put the interests of children and their protection before financial gain.
- Providing the possibility of removing images of children from the Internet, such as images of victims of sexual blackmail, if they are published on the Internet, and allowing victims to report anonymously without revealing their identity, and preventing them from being uploaded to platforms.
- The necessity of imposing digital awareness in schools at all ages, and all media, and teaching the child how to protect himself and refer to his parents in the event of being exposed to electronic blackmail without fear or anxiety from them.
- Use artificial intelligence to monitor suspicious actions and analyze unlawful content, and take advantage of artificial intelligence technology to efficiently analyze suspicious behaviors and detect illegal content, which adds to improved cybersecurity.
- The need to constantly improve dark web monitoring technologies in order to discover cyber dangers early and respond to them effectively, hence reducing future risks.
- International collaboration must be strengthened to prosecute perpetrators of dark web crimes by establishing collaborative agreements between countries that facilitate the interchange of information and resources to pursue cybercrimes on the dark web.
- The need to increase digital awareness in order to eliminate digital literacy among children and parents, through awareness programs aimed at raising understanding

of electronic protection mechanisms as well as how to spot suspicious messages and deal with them efficiently.

References

Abdel-Ati, Muhammad Saeed and Al-Minshawi, Muhammad Ahmad. (2021), The Role of Criminal Law in Protecting Children from Electronic Blackmail (A Comparative Study). Al-Azhar University, Faculty of Sharia and Law, Journal of Jurisprudential and Legal Research, 33 (36), pp. 123–178. https://jlr.journals.ekb.eg/article_200366.html.

Abdul Manap, N., & Aljuboori, O. (2024). LEGAL PROTECTIONS FOR VICTIMS OF CYBER BLACKMAIL IN THE Republic of Iraq, THE United States, AND Malaysia. Malaysian Journal of Syariah and Law, 12(2), 334–349. https://doi.org/10.33102/mjsl.vol12no2.657.

Al-Ajami, Raja. (10-08-2024). The psychological effects of electronic blackmail reach the point of nervous exhaustion and suicide, alwatannews. https://alwatannews.net/Specialist/%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A9/article/1119642/%D8%A2%D8%AB%D8%A7%D8%B1-%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%A7%D9%84%D9%86%D9%81%D8%B3%D9%8A%D8%A9-%D8%AA%D8%B5%D9%84-%D8%AD%D8%AF-%D8%A7%D9%84%D8%A7%D8%AD%D8%AA%D8%B1%D8%A7%D9%82-%D8%A7%D9%84%D8%B9%D8%B5%D8%A8%D9%8A-%D9%88%D8%A7%D9%84%D8%A7%D9%86%D8%AA%D8%AD%D8%A7%D8%B.

AI-Khazaleh, M. S. & Lahiani, H. (2023). Cybercrime and harassment: the impact of blackmailing on Jordanian society as a case study. *Journal of Intercultural Communication, 23*(3), pp. 116–123.

Alkhalil Z, Hewage C, Nawaf L & Khan I (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science. 3 (563060). https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full.

Al-Tahhan, Zainab, (2024). Electronic blackmail. its severity is increasing, and a new method involves the victim in hacking her accounts, Children's Safety. https://www.amankids.com/post/16079/.

Amankids. (n. d.). Child Victims Are a Commodity on the Dark Web; What Is It and What Technology Can Protect Us from It? Date of Access: October 3, 2024. https://www.amankids.com/post/16687/.

Abu Amshah, Esraa F. M., (2024). The Dangers of the Internet to Children and Proposed Mechanisms to Protect Them from It, The 8th Annual International Educational Conference. https://www.jaesjo.com/index.php/conf/article/view/778.

Axelton, Karen. (24-08-2022). 11 Common Scams Targeting Children and Teens, Experian. https://www.experian.com/blogs/ask-experian/common-scams-targeting-children-teens/.

Bergman, Jesper & Popov, Oliver B. (2023) "Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation," in *IEEE Access*, vol. 11, pp. 35914–35933. https://ieeexplore.ieee.org/document/10064292.

Carle, N., & Ophoff, J. (2024). Using Visual Cues to Enhance Phishing Education for Children. In: Drevin, L., Leung, W.S., von Solms, S. (eds) Information Security Education—Challenges in the Digital Age. WISE 2024. IFIP Advances in Information and Communication Technology, vol 707. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-031-62918-1_2.

Chertoff, Michael. (2017). A public policy perspective of the Dark Web, Journal of Cyber Policy, 2(1), pp. 26–38. https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643#abstract.

Daradkeh, Y., & Abu Asaad, A. (2023). The Effectiveness of a Preventive Group Counseling Program for not Being Exposed to Electronic Extortion and Addiction to Electronic Games among Students of the Upper Basic Stage. Educational and Psychological Sciences Series, *2*(3), 431–465. https://journals.aabu.edu.jo/index.php/Edu/article/view/289.

Egan, Matt. (2019, 01 30). What is the Dark Web & How to Access it? Retrieved 07 23, 2019, from. https://www.techadvisor.co.uk/how-to/internet/darkweb-3593569/.

Ferrara P, Franceschini G, Corsello G, Mestrovic J, Giardino I, Vural M, Pop TL, Namazova-Baranova L, Pettoello-Mantovani M. (2021). The Dark Side of the Web-A Risk for Children and Adolescents Challenged by Isolation during the Novel Coronavirus 2019 Pandemic. J Pediatr, 228:324–325.e2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7547580/.

Finklea, K. M. (2015). Dark web, Congressional Research Service, pp. 1–16.

Gehl, Robert. (2014). Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network. New Media and Society, Forthcoming. https://ssrn.com/abstract=2498629.

Get Cyber Safe, (04-01-2022). How (and what) to teach your kids about phishing, Government of Canada. https://www.getcybersafe.gc.ca/en/blog/teach-kids-about-phishing.

Hussein, Omar Abdulsalam, Manap, Nazura Abdul, Abdul Rahman, Muhammad Rizal, (2022). Cyber Blackmail Crime Against Women—A Case Study, Journal of Positive School Psychology, 6(3), pp. 6882–6893. https://journalppw.com/index.php/jpsp/article/view/4224.

Kaspersky (n.d.). The dark side of kids' virtual gaming worlds, available at. https://www.kaspersky.com/blog/threats-in-kids-gaming-worlds/.

Kastner, Erica (02-07-2020). History of the Dark Web [Timeline], SOScanhelp https://www.soscanhelp.com/blog/history-of-the-dark-web.

Kavenagh, M. (2023, November 17). Child Sexual Exploitation in Online Gaming, Risks and Realities, UNICEF. https://www.unicef.org/eap/blog/child-sexual-exploitation-online-gaming.

Keeper. (2024). https://www.keepersecurity.com/ar_AE/threats/what-is-phishing.html.

Kumar, Naveen, (2021). CHILDREN AND CYBER CRIMES, International Journal of Social Science and Economic Research, 6(4), pp. 1324–1334. https://ijsser.org/more2021.php?id=85.

Li Z, Du X, Liao X, Jiang X, Champagne-Langabeer T, Demystifying the Dark Web Opioid Trade: Content Analysis on Anonymous Market Listings and Forum Posts, J Med Internet Res 2021; 23(2), pp. 1–16. https://doi.org/10.2196/24486.

Makkawi, Muhammad Hassan, (2022). Electronic blackmail between threat and protection: A study in Egyptian and American legislation, Journal of Law and Emerging Technologies, 2(2), pp. 53–116.

Marouf, Reham Atef, (2023). Electronic Blackmail, The Eighth International Scientific Conference—Technology and Law, Journal of the Spirit of Laws—Faculty of Law—Tanta University, 35(102), pp. 1995–2018. https://las.journals.ekb.eg/article_343891.html.

Ofusori, L. O., & Hendradi, R. (2023). Understanding the Impact of the Dark Web on Society: A Systematic Literature Review. International Journal of Information Science and Management, 21(4), 1–21.

Qarinh, Fatima Zahra, Rashid, Kamal, (2011). Protecting children from the crime of electronic threat between international and Algerian legislation, Journal of Law and Society, 9(2).

Samurai security, (18-03-2024). The Dark Web's Effect on Children: BBC Interview with Dr. David Day. https://samuraisecurity.co.uk/resources/in-the-media/dark-web-effect-on-children-interview/.

Security fingerprint. (n.d.). Blackmailing children through social media and their lives. https://www.secprint.sa/blackmailing-children/.

Sjouwerman, S. (2018, December 21). Children's Full Personal Data and SSNs Are Being Sold on the Dark Web. KnowBe4. https://blog.knowbe4.com/childrens-full-personal-data-and-ssns-are-being-sold-on-the-dark-web.

Sönmez, Eda & Codal, Keziban Seckin, (2021). Terrorism in Cyberspace: A Critical Review of Dark Web Studies under the Terrorism Landscape, Sakarya University Journal of Computer and Information Sciences 5(1). https://www.researchgate.net/publication/357156317_Terrorism_in_Cyberspace_A_Critical_Review_of_Dark_Web_Studies_under_the_Terrorism_Landscape.

TAHER, KARRAR ABDULRIDHA. (2024). Electronic Extortion "Challenges and Solutions", Kut University College Journal for Humanitarian Science, 5(1), pp. 89–97. https://www.iasj.net/iasj/article/314892.

The guardian, (2024). 'It looks so real': amid rise in financial sextortion, Childline is helping teenagers fight back. https://www.theguardian.com/uk-news/article/2024/aug/21/amid-rise-in-financial-sextortion-childline-is-helping-teenagers-fight-back.

Trevino, (13-07-2023). Is the Dark Web Dangerous? Keeper. https://www.keepersecurity.com/blog/2023/07/13/is-the-dark-web-dangerous/.

Vallance, Chris. (23-04-2024). Three-year-olds groomed online, charity warns, BBC News. https://www.bbc.com/news/articles/cx9wezr1d1vo.

Yassin, Ben Omar, (2024). Electronic blackmail of children in Algerian legislation, DSpace at Kasdi Merbah University Ouargla, 16(2), pp. 169–183. https://dspace.univ-ouargla.dz/jspui/handle/123456789/36416.

Combating Child Sexual Exploitation on the Dark Web: Technical, Legal, and Psychological Perspectives



Ramy El-Kady

1 Introduction

Technology has become a double-edged sword. Criminals use it to engage in illegal activities, and law enforcement agencies use it to track these activities and arrest their perpetrators. This mutual dependence on technology underscores the need for robust and extensive collaboration between law enforcement agencies and technology on an international scale. The global nature of these crimes necessitates and underscores the need for international collaboration, which is crucial in finding solutions that help law enforcement agencies prosecute criminals and apply justice.

Rapid technological advancements have enhanced the work methods for criminals and organized criminal groups, leading to their evident Internet exploitation. With its vast reach and anonymity, the Internet has opened up new avenues for illegally buying and selling goods, whether through the visible web or the Darknet (El-Kady 2024). This rapid evolution necessitates continuous adaptation and innovation in law enforcement strategies to combat these crimes effectively.

Criminal and terrorist organizations seek to take advantage of the dark web, especially its secret nature and the difficulty of tracking its users, to enable them to directly carry out their criminal activities away from any legal control or accountability, as there are sites on this network those sell forged and stolen documents, credit card data, and personal accounts. This network has become a black market for all illegal activities and a breeding ground for criminals, hackers, hired killers, counterfeiters, human traffickers, etc. Hence, any user on the network communicates with them to obtain these services in complete secrecy without being exposed to official censorship (El-Kady et al. 2025).

Reports and studies have underscored the gravity of criminal activities on the dark network. The circulation of artistic works and programs through the dark network

R. El-Kady (✉)
Dubai Police Academy, Dubai, United Arab Emirates
e-mail: ramy_elkady@alumini.cu.edu.eg

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_10

in 2005 caused losses to commercial companies—at that time—estimated at 34 billion US dollars worldwide. Another report indicated that the profits of the Silk Road website, established in 2011 for drug promotion, were estimated at $1.2 billion during 2011–2013. One study also revealed that electronic fraud via the dark network costs the British economy tens of billions annually (El-Kady 2024).

Not to mention what one cybersecurity company announced that the black network in 2010 now included more than 50,000 websites for extremist ideology and more than 300 virtual forums for terrorist groups, in addition to these organizations' use of profits from selling stolen software to finance terrorist operations, in addition to that. I was using this network to establish communications between members of extremist terrorist organizations (El-Kadyet al. 2025).

It is worth noting that these criminal activities are practiced by criminal organizations that are professional in crime, characterized by stability and permanence in their composition, aim to achieve profit, and operate on a broad international scale, including many countries, in addition to their use by extremist terrorist elements. There is no doubt that this constitutes a danger. It is a significant threat to all societies' security and requires concerted international efforts to confront it.

This is in light of the opportunities that the use of the Internet provides for cybercriminals to commit crimes outside the scope of their countries, in addition to facilitating the process of communication and exchange of information between them, which enables them to meet in the virtual world, and plan and prepare to commit their crimes, the scope of which extends to more than one country. Sometimes, these organized criminal groups may target specific countries or commercial or economic institutions, which may lead to severe economic damage to these countries or institutions (El-Kady et al. 2024).

This research aims to achieve a primary goal, which is to shed light on the use of the dark web by criminal and terrorist organizations; this can be achieved through a group of sub-objectives, the most prominent of which is shedding light on illegal criminal activities through the dark web, and examining ways to combat it in light of the related technical and legal challenges, the role of national legislation in limiting these activities, the role of international police agencies in tracking them, and the best scenario for dealing with them.

The central hypothesis of the study is that there are practical obstacles and difficulties in confronting crimes committed on the Dark Web due to the high encryption techniques used in this network, which has made this network a black market for many illegal activities and facilitates criminals to commit their crimes away from the hands of law enforcement agencies, in addition to the difficulty of extending These entities monitor this network to achieve their preventive role in preventing crimes from occurring.

2 Literature Review

Research indicates that the dark web enables severe criminal activities targeting children, leading to hazardous conditions for exploitation and abuse. It entails intricate offender behaviors and security measures. The dark web has emerged as a prominent venue for enabling crimes against minors, such as sexual exploitation and abuse. The clandestine realm of the internet provides a platform for wrongdoers to carry out their activities without revealing their identities, posing a formidable obstacle for law enforcement agencies in their efforts to monitor and capture them. The detrimental impacts on children are significant, encompassing psychological distress and enduring emotional and physical damage. The dark web greatly amplifies the issue of child sexual exploitation by offering a medium for perpetrators to engage in illegal activities without revealing their identities and across national borders. Some studies suggest establishing trust among users and the particular actions and measures perpetrators take to emphasize the intricacy of combating these crimes. To effectively combat the issue, it is necessary to adopt a comprehensive strategy that involves international collaboration, innovative technical interventions, and a thorough grasp of psychology and criminology (El-Kady and Uddin 2024).

Several studies indicate that the dark web facilitates the activities of individuals who exploit children, allowing them to search for victims and trade illegal materials across international boundaries. This poses challenges for conventional law enforcement methods. Some scholars recognize that computer-facilitated crimes against minors are a significant worldwide issue, as the dark web has emerged as a new platform for abusers to target victims and trade illicit materials (Geldenhuys 2017).

Another study offers valuable information regarding suspect profiles, motivations for utilizing the Dark Web, criminal behavior, technical and security measures used, sexual interests, and their interactions (Woodhams et al. 2021). Some scholars observe that users of dark web portals specifically designed for child exploitation establish trust and connections in order to justify, normalize, and encourage their actions. Despite the high-risk setting, these exchanges offer access to expert counsel and materials. The Dark Web networks function as hazardous and high-stakes venues for the exploitation and abuse of children, where users have difficulties in establishing confidence and dealing with potential dangers (Kloess and Bruggen 2023).

Observers note that individuals involved in illicit activities on the dark web have distinct attributes and actions, such as careful attention to technological and security measures, distinctive motivations, and particular sexual preferences. Their conversations frequently entail the exchange of information and tactics to evade detection (Woodhams et al. 2021).

In the same context, additional research is observed. A novel social learning technique is suggested to combat online child sexual abuse to diminish juvenile misbehavior on the dark web (Yang et al. 2022). Another study shows that Law enforcement organizations utilize OSINT (Open-Source Intelligence) on the Dark Web to investigate crimes involving child abuse content, effectively tackling issues associated with data preservation and criminal investigation (Rajamäki et al. 2022).

A study shows that excessive utilization of digital media in children and adolescents is linked to inadequate sleep, behavior related to ADHD, and reduced ability to cope socially (Lissak 2018). The Dark Crawler has effectively located and retrieved data about child exploitation photographs, videos, and connections on the public internet (Zulkarnine et al. 2016). One of the studies emphasizes the necessity for further comprehensive investigation into criminal concerns on the Dark Web, including targeting cryptocurrency markets and discussion forums for forensic examinations. It also underscores the utilization of anonymity as a tool to apprehend wrongdoers and dismantle unlawful websites (Nazah et al. 2020). One study shows that Children's well-being is adversely impacted by internet usage, specifically harming their self-perception of their physical attractiveness (McDool et al. 2020).

3 Methodology

The most prominent research problems crystallize in the unique technical nature required to deal with this dark network to access it and monitor and follow up on its illegal activities as a result of the difficulty of accessing it through traditional search engines and the use of complex encryption techniques, which work to anonymize its users and make identification difficult. On them, track them, and control them.

The descriptive-analytical method is the most appropriate research method for studying social and legal phenomena. It emphasizes the examination of the phenomenon as it manifests in reality, providing a detailed description and articulating it either qualitatively or quantitatively to derive conclusions that enhance comprehension and advancement of this reality. Also, the research subject and its transnational character require the author to use a comparative approach, referring to some facts and incidents related to organized crime activities via the dark web and focusing on the position of the Egyptian legislator on confronting these dangerous criminal phenomena.

The descriptive-analytical method is the most suitable research method for studying dark web crimes, as it involves closely describing and expressing the phenomenon, using a comparative approach to compare facts and incidents. The research tools that the author will use as scientific sources in preparing this research are the legal literature discussing the topic of study in the scope of criminal law and the relevant specialized literature, whether they are books, papers, etc., or doctoral dissertations. Alternatively, a master's degree or legal articles on the topic are published in scientific journals.

4 Discussions

The chapter is divided into four main parts. The first part presents Child trafficking and child abuse as the most prominent crimes committed on the dark web. The second part concerns international and national efforts to control dark web crimes against children. The third part presents Cutting-edge technologies for detecting CSE on the dark web. The fourth part discusses preventive strategies for Combating CSE on the Dark Web.

Part One- Child Trafficking and Child Abuse as the Most Prominent Crimes Committed on the Dark Web

Introduction of the Dark Web:

The dark web is an internet-based network. To access it, one must have the appropriate software and configure one's Internet-capable equipment (Gannon et al. 2023). The global internet has a daily user base of 5.07 billion individuals (Datareportal 2022). Although the dark web's daily user base represents a mere 0.04% of the total number of daily Internet users, it nonetheless encompasses approximately 2.5 million users every day (Wise 2022).

The Internet emerged in the late 1990s and became integral to our daily routines in 2004. By 2018, 90% of households were connected to the Internet (Martin 2021), with most European countries reporting similar percentages (Eurostat 2022). The surge in popularity was facilitated by technological advancements, including the availability of hardware and software that enabled fast and reliable data transfer and storage. The Internet transformed from a medium for publishing to a medium for active participation, where users can connect, engage, and generate content in emerging virtual communities.

The widespread adoption of the Internet has led to a demand for anonymous online communications, particularly for military personnel, journalists, and individuals representing political and religious minority groups in autocratic governments. The United States Navy created the initial models for The Onion Router (TOR) in the 1990s to fulfill this requirement. In 2002, TOR was made accessible to the public, offering a vast network of servers to conceal user identities. TOR employs encryption to obfuscate web traffic, redirecting the user's IP address through randomly selected servers (Gannon et al. 2023).

The TOR browser, which functions as an Internet browser, allows users to access the World Wide Web while guaranteeing their privacy. It supports darknet sites, onion sites, and online platforms with URLs ending in onion. These sites, known as "hidden services" or HSes, are not searchable by commonly used search engines. Despite its contribution to social movements, the anonymity of the TOR network also facilitates a wide range of illegal marketplaces, such as Silk Road and Alphabay. These platforms replicate the operations of legitimate online marketplaces like eBay, allowing vendors to promote their products and provide escrow services to buyers who make

transactions using Bitcoin or other cryptocurrencies. Additionally, many marketplaces provide chat rooms for vendors and customers to interact, share experiences, and offer feedback and guidance to fellow online community members (Gannon et al. 2023).

The Risks of the Dark Web on Children:

Some studies indicate that the dark web presents substantial dangers to children, such as the potential for encountering child sexual abuse content, direct communication with criminals, and the enabling of sexual crimes. The dark web, an unindexed portion of the internet that necessitates specialized software for access, has been increasingly linked to a range of illicit endeavors, particularly those that endanger minors. Based on various research findings, this synthesis analyzes the possible hazards the dark web poses to children. The dark web presents substantial dangers to children, mainly by enabling child sexual exploitation and abuse, exposing them to hazardous content, and increasing the probability of online grooming and contact with unfamiliar individuals. These concerns emphasize the necessity for improved preventive measures and knowledge to protect children from the hazards of the dark web.

Several studies have found that the dark web facilitates the connection and interaction of individuals who have a sexual attraction to children, allowing them to participate in unlawful acts. It serves as a platform for the exchange of child sexual abuse material (CSAM) and the establishment of trust among offenders. The Dark Web is a challenging and hazardous network where users must navigate constant threats and have limited knowledge about others and their reliability (Kloess and Bruggen 2023).

Additional research demonstrates that children who utilize social networking sites are exposed to more online hazards than those who do not. The level of danger encountered varies based on the precise relationship between the hazards and the platforms used, such as websites, instant messaging, gaming, or social networking (Staksrud et al. 2013).

A recent study has demonstrated that over 50% of individuals who look for CSAM (Child Sexual Abuse Material) on the dark web actively seek direct communication with children online. This finding suggests a significant likelihood of shifting from mere consumption of unlawful information to engaging in actual acts of abuse. The data demonstrates that 42% of participants actively sought direct interaction with minors online after accessing child sexual exploitation material on the dark web (Insoll et al. 2022).

Additional research substantiates that children who are exposed to violent and pornographic material online, even via dark websites, frequently encounter feelings of shock, revulsion, and terror, which can result in enduring psychological consequences. Children express apprehensions over pornography, potential dangers such as cyberbullying, and the presence of violent content on the internet (Livingstone et al. 2014).

Several studies have demonstrated that the utilization of social media and other internet platforms, which are accessible through the dark web, is linked to a range

of adverse outcomes for children, such as sadness, anxiety, and behavioral issues. The utilization of social media among children and adolescents is linked to various concerns, including melancholy, anxiety, sexual matters, behavioral difficulties, and other connected problems (Bozzola et al. 2022). Another study shows that the primary discoveries of the investigation encompass intergenerational conflicts and the challenge of attaining agreement on the secure utilization of the Internet for youngsters and adolescents (Núñez-Gómez et al. 2021).

Several studies indicate that the dark web enables communication between criminals and children, hence heightening the likelihood of online grooming and sexual solicitation. Less than 20% of adolescents are often affected by the risks of cyberbullying, interaction with strangers, sexual texting (also known as "sexting"), and exposure to pornography (Livingstone and Smith 2014). Additional study indicates that online hazards such as addiction, cyberbullying, and sexual solicitation have detrimental effects on young people (Guan and Subrahmanyam 2009).

Additional research indicates that children who utilize social networking platforms are more likely to encounter online hazards, such as interacting with unfamiliar individuals. These hazards can be intensified by the anonymity and absence of regulation on the dark web. Children who engage in social networking sites face more online hazards than those who do not. The level of risk varies depending on the precise relationship between risks and platforms, such as websites, instant messaging, gaming, or social networking (Staksrud et al. 2013).

Child Trafficking on the Dark Web:

Child trafficking involves the exploitation of both girls and boys, primarily for forced labor and sexual exploitation. Approximately 27% of all human trafficking victims globally are children, with females making up two-thirds of child victims. Occasionally, these children are sold by a relative or someone they know, while other times, they are enticed by deceitful assurances of education and an improved existence.

However, the truth is that these children who are trafficked and exploited endure conditions akin to slavery, lacking sufficient sustenance, shelter, and clothing. Moreover, they frequently suffer severe abuse and are completely isolated from their families. Children are frequently subjected to trafficking for commercial sexual exploitation or various forms of labor, including domestic slavery, agricultural work, factory work, mining, or even being coerced into participating in armed wars. Refugees and migrants, especially the most vulnerable children, are frequently targeted and exploited, undermining their aspirations for education, improved employment opportunities, or a better life in a foreign nation (El-Kady 2024).

Several studies indicate that the Dark Web enables child exploitation and abuse by offering platforms for communication, validation, and exchange of illicit materials, as well as by establishing virtual communities that endorse and promote these acts. The Dark Web, an unindexed section of the internet that necessitates specialized software for access, has been recognized as a prominent platform for promoting child exploitation and abuse.

This synthesis investigates the degree to which the Dark Web contributes to these illicit activities based on various research findings. The Dark Web significantly enables child exploitation and abuse by offering a platform for individuals to meet, interact, and share unlawful material anonymously. The chronic and complex issue arises from the structure, dynamics, and challenges law enforcement faces in dealing with these networks. In order to effectively address these actions, it is crucial to consider the distinct attributes of the Dark Web and the necessity for specialized investigative methods.

Many scholars observe that the Dark Web facilitates the gathering of persons who have a sexual attraction towards children, allowing them to connect, communicate, and participate in unlawful actions. This platform serves as a means of affirmation, acceptance, and encouragement for individuals with similar interests. Dark Web networks enable the perpetration of child sexual exploitation and abuse by offering affirmation, normalcy, assistance, and access to specialized guidance and knowledge (Kloess and Bruggen 2023).

Other scholars state that the Dark Web enables the exploitation and mistreatment of children by offering a medium for individuals to discuss and exchange unlawful materials related to child pornography (Fonhof et al. 2019). A recent study indicates that the deep web has been utilized for engaging in criminal and illicit activities, such as child sexual exploitation (Kumar 2021).

A study has provided evidence that Online child exploitation networks operating on the Dark Web are organized in a manner that facilitates the sharing of unlawful child pornography content. Law enforcement agencies are particularly interested in identifying the prominent individuals involved and understanding the structure of these networks (Fonhof et al. 2019). A recent study has provided further evidence that the Dark web has a significant impact on the methods used to perpetrate crimes involving child sexual exploitation material (CSEM) (Van Der Bruggen and Blokland 2022).

Many researchers argue that the Dark Web's anonymous character poses challenges for law enforcement organizations in tracking and prosecuting criminals. These platforms let users conceal their identities while engaging in activities such as sharing information, trading goods, and providing services. The Dark Web has emerged as a new platform where those who exploit children actively search for victims and exchange illicit materials, posing a significant challenge to conventional law enforcement efforts (Geldenhuys 2017).

Another scholar perceives the Dark Web as a conducive setting for the illicit transmission of information, goods, and services (Rajamäki et al. 2022). Some researchers argue that The Dark Web, mainly through platforms like The Pirate Bay, facilitates the dissemination of millions of instances of child sexual abuse content with minimal concern for legal consequences (Broadhurst and Ball 2021). Some experts argue that the investigation of child sexual abuse material (CSAM) on the Dark Web encounters notable obstacles, such as difficulties in storing data and the requirement for law enforcement officials to undergo specific training (Rajamäki et al. 2022).

Some experts argue that Dark web markets enable the trading of child sexual abuse material (CSAM), as evidenced by the discovery of 724 CSAM items in two Chinese

markets, while no such goods were found in mainstream English markets (Wang et al. 2023). Some experts argue that the establishment of trust and relationships between users of Dark Web child exploitation networks is essential for the operation of these communities.

This is because users have to navigate risky situations with little knowledge about the trustworthiness of others (Kloess and Bruggen 2023). Others argue that analyzing the communication patterns of forum users can help law enforcement identify individuals who are highly influential and constitute a significant risk in internet forums related to child sexual exploitation material (Bruggen and Blokland 2021).

Some experts argue that these societies are frequently linked together through linkages, creating stable networks that enable the distribution of child sexual exploitation content. Child sexual exploitation networks create online communities where individuals frequently link to each other's content more often than they do with the rest of the network (Westlake and Bouchard 2016).

Some experts have observed the spread and commercialization of CSAM (Child Sexual Abuse Material) on the Dark Web. Notably, specific markets, especially in the Chinese context, have shown substantial activity and sales in this regard (Wang et al. 2023). Others see that, despite attempts to mitigate the dissemination of Child Sexual Abuse Material (CSAM), it continues to be widespread on the Dark Web, intensified by the anonymity and unrestricted nature of these platforms (Broadhurst and Ball 2021).

Legal Framework to Combat CSE on the Dark Web:

The dark web presents significant challenges in combating child sexual exploitation due to its anonymity and the global nature of the internet. Various legal frameworks and international collaborations are essential to address this issue effectively. A few studies suggest that the legal framework to combat child sexual exploitation on the dark web requires international legislation, concerted law enforcement efforts, and compliance with international legal standards.

Scholars show that most countries have laws protecting children, but there is a need for concerted international law enforcement and legislation to combat child sex abuse effectively. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is a step towards this in Europe. Otherwise, according to Kierkegaard, The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse may help combat child sexual exploitation in Europe (Kierkegaard 2008). Besides the Budapest Convention on Cybercrime, this is highlighted as a significant international legal framework for combating cybercrimes.

In the same context, others see that detecting online child sexual exploitation is more challenging than offline cases. There is often a significant gap between reported and actual cases due to various factors, including the difficulty of detection and the lack of comprehensive statistics. That is what Dushi tried to explain in his study by analyzing international legal instruments and evaluating Kosovo's legislation in the fight against online sexual exploitation of children, drawing recommendations for future development (Dushi 2018).

Furthermore, others identified that users of dark web networks dedicated to child sexual exploitation engage in interpersonal communication to validate, normalize, and support their activities. These networks are high-risk environments where trust and relationship development are crucial for users to navigate threats and maintain anonymity (Kloess and Bruggen 2023).

In conclusion, combating child sexual exploitation on the dark web requires robust international legislation and cooperation, as well as effective detection and enforcement mechanisms. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is a significant step forward. However, challenges remain in detecting and addressing these crimes due to the nature of the dark web and the need for trust among perpetrators. Enhanced international collaboration and improved detection strategies are essential to bridge the gap between reported and actual cases.

Psychological Impacts of Exposure to Dark Web Crimes on Children:

Some studies indicate that being exposed to criminal activities on the dark web can result in secondary traumatic stress, diminished well-being, heightened anxiety, decreased self-esteem, and reduced social competence in youngsters. Children who are exposed to crimes on the dark web, especially those related to child exploitation, might experience significant psychological consequences. This compilation of scholarly articles examines the diverse aspects of these effects.

Children who are exposed to crimes on the dark web, particularly those related to child exploitation, experience significant psychological consequences. These effects encompass heightened anxiety, diminished self-worth, and elevated tendencies towards impulsive and deviant actions. Furthermore, those employed in this particular industry also encounter substantial secondary traumatic stress. Normalizing and validating detrimental actions within dark web networks intensify these problems.

Research indicates that those who are engaged in the investigation of cybercrimes against children, such as members of the ICAC task force, undergo considerable levels of secondary traumatic stress as a result of their exposure to child exploitation and sexual abuse. Being exposed to child exploitation and sexual assault can lead to secondary traumatic stress, which can have a negative influence on both personal and professional well-being (Bourke and Craun 2014).

Another research indicates that Children and adolescents who are victims of cyberbullying report reduced psychological well-being, which manifests as heightened anxiety, diminished self-esteem, and increased tendencies towards impulsivity and deviant behaviors. These adverse consequences are interrelated and might intensify one another. Cyber victimization is correlated with diminished well-being, heightened anxiety, diminished self-esteem, and reduced social competence in children and adolescents (Audrin and Blaya 2020).

Research findings indicate that dark web platforms specifically designed for child exploitation offer a location where users can engage with others who share similar interests, reinforcing and normalizing their activities. This context can sustain detrimental behaviors and attitudes, intensifying the psychological effects on individuals

who engage in harmful actions and those subjected to them. Participating in interpersonal conversation and engaging with like-minded individuals in Dark Web networks provides validation, normality, support, and the opportunity to obtain professional guidance and information (Kloess and Bruggen 2023).

In a similar context, additional research indicates that children's mental and emotional well-being can be impacted by their exposure to extreme violence and terrorism in the media, with specific children being more susceptible to adverse impacts (Leiner et al. 2016). Another study shows that being exposed to child pornography results in the development of secondary trauma symptoms and has an impact on parenting behaviors, specifically in the case of mothers (Stewart and Witte 2020). A third study shows that children who are exposed to acts of terrorism, mainly through media coverage, can develop post-traumatic symptoms (Pereda 2013).

Another research shows that being exposed to dark web crimes can result in psychological stress, becoming a victim, and experiencing harassment. The individuals responsible for these crimes often exhibit narcissistic behavior, self-centeredness, and passive-aggressive self-assertion (Tzokov 2019). Another scholar shows that excessive utilization of digital media among children and adolescents is linked to inadequate sleep, indications of depression, and behavior related to ADHD (Lissak 2018).

A study offers valuable information regarding suspect profiles, their reasons for utilizing the Dark Web, their criminal activities, their measures to protect themselves, their sexual preferences, and the content of their online interactions (Woodhams et al. 2021). The borderless nature and constantly evolving technology of dark web crimes present a significant challenge to traditional law enforcement (Geldenhuys 2017).

Psychological Effects of Cyber Victimization on Children:

Research indicates that children who experience cyber victimization are more likely to exhibit symptoms of heightened anxiety, despair, diminished self-worth, reduced social and academic abilities, feelings of isolation, internalizing and externalizing difficulties, as well as violent behaviors. Cyber victimization, which refers to the deliberate targeting of individuals through digital platforms, is now widely acknowledged as a significant concern that negatively impacts the mental health of children.

This synthesis investigates the psychological impacts of cyber victimization on children, drawing on several research papers. Cybervictimization has significant and diverse psychological impacts on children. Victims frequently encounter heightened levels of anxiety, despair, and solitude, along with diminished self-worth and social proficiency. The psychological effects can result in aggressive behaviors, physical problems, and academic challenges. To effectively combat cyber victimization, it is necessary to implement comprehensive interventions that prioritize mental health and social-emotional development in order to reduce the negative consequences.

A study indicates a strong correlation between Cyber victimization and heightened levels of anxiety and depression in children and adolescents (Audrin and Blaya 2020). Another study has demonstrated that there is a reciprocal association between cyber victimization, sadness, and anxiety in school-aged kids (Rose and Tynes 2015).

A recent study has provided further evidence that cyber victimization is linked to heightened levels of anxiety ($r = 0.31$) and depression ($r = 0.28$) among teenagers, hence exerting a negative impact on their overall development (Molero et al. 2022).

A recent study has provided further evidence of a reciprocal association between anxiety and depression, which can both serve as predictors and be predicted by cyber victimization over some time (Rose and Tynes 2015). Another study has provided further evidence that children who are victims of cyberbullying frequently exhibit decreased self-esteem and worse social skills, which can manifest as heightened impulsivity and engagement in deviant behaviors (Audrin and Blaya 2020).

A recent study has provided further evidence that cyber victimization is directly and negatively associated with self-concept and school anxiety while also being directly and positively associated with aggressiveness. It has demonstrated a direct correlation between Cyber victimization and increased levels of loneliness and social anxiety, especially among children who possess a heightened sensitivity to social interactions (Escortell et al. 2020).

A recent study has demonstrated that cyber victimization is inversely correlated with school competence and academic progress and positively correlated with loneliness in children, particularly those with heightened social sensitivity (Li et al. 2021a, 2021b). Another research indicates that individuals who have been targeted by cyberbullying are more likely to display heightened levels of aggression, particularly when they have experienced relational victimization. It indicates that individuals who have been targeted by cyberbullying are more likely to display heightened levels of aggression, particularly when they have experienced relational victimization (Escortell et al. 2020).

A study indicates that there is a correlation between experiences of cyber victimization and traditional victimization with the development of internalizing symptoms and violent behaviors in elementary school students (Holfeld and Leadbeater 2018). Another study indicates that Cyber victimization is linked to both psychological and physiological symptoms, such as headaches and stomachaches, suggesting a broader influence on general health. There is a positive correlation between cyber victimization and the occurrence of psychological and somatic symptoms in both male and female pupils (Vieno et al. 2015).

A study reveals a negative association between cyber victimization and academic performance, as children affected by cyber victimization tend to exhibit lower levels of school competence and achievement (Li et al. 2021a, 2021b). Studies indicate that children who are victims of cyberbullying, particularly those who do not also experience traditional bullying, exhibit a higher prevalence of conduct difficulties and externalizing behaviors.

Some scholars indicate that individuals who are targeted by cyberbullying but not traditional bullying experience more significant challenges in terms of conduct problems, externalizing problems, adverse effects on their home life, and overall difficulties as measured by the SDQ scales (Sidera et al. 2021). Additional research indicates that Peer cyber victimization is linked to internalizing issues such as depression, anxiety, and anger, as well as externalizing problems, including violence and engaging in risky sexual activity among adolescents (Fisher et al. 2016).

Psychological and Criminological Factors Contributing to CSE on the Dark Web:

Some studies indicate that psychological and criminological elements influence child sexual exploitation networks on the Dark Web. These aspects include validation and support gained through connections, various risk factors such as abuse and poverty, and the impact of multiple theoretical frameworks. The utilization of children on the Dark Web is a multifaceted problem driven by a range of psychological and criminological elements.

A comprehensive understanding of these characteristics is essential for formulating efficient preventative and intervention methods. The Dark Web child exploitation networks are influenced by psychological and criminological elements such as the establishment of trust and relationships between users, the presence of vulnerability features in minors, and the application of typical criminal career dimensions in online settings. Gaining insight into these issues using appropriate frameworks and theories is crucial for developing effective strategies for prevention and intervention.

Some researchers see that Dark Web child exploitation network users engage in interpersonal conversation to justify, normalize, and support their acts and get professional guidance and materials. Trust is essential in these high-risk contexts, as users must consistently handle threats and evaluate the reliability of others. Participating in interpersonal conversation and engaging with like individuals in Dark Web networks provides validation, normality, support, and the opportunity to obtain professional guidance and information (Kloess and Bruggen 2023).

Some scholars argue that numerous risk factors make children more susceptible to sexual exploitation. These factors include child abuse, caregiver strain, running away, substance use, peer influence, witnessing family violence, poverty, academic difficulties, conflicts with parents, poor mental health, involvement in child protective services, juvenile detention, early substance use, and previous instances of sexual victimization.

Relevant frameworks for comprehending risk factors in child sexual exploitation encompass the life-course viewpoint, ecological model, multilevel model, ecodevelopment model, traumatic variables, and general strain theory. They observe that various factors contribute to the risk of child sexual exploitation, such as child abuse, maltreatment, caregiver strain, running away, substance use, peer influence, witnessing family violence, poverty, academic difficulties, parental conflict, poor mental health, and involvement in child protective services (Franchino-Olsen 2021a, 2021b).

They also observe that several frameworks and theories are used to understand the vulnerabilities contributing to child exploitation. These include the life-course viewpoint, ecological model, multilevel model, ecodevelopment model, traumatic variables, and general strain theory. These frameworks delineate the interconnections and mechanisms of risk factors, facilitating focused preventive endeavors (Franchino-Olsen 2021a, 2021b).

Some researchers believe that traditional criminal career parameters, such as the amount of illicit content and the popularity of the website, may predict the survival or

failure of child exploitation websites. Websites with more CE code words and images are at a greater risk of experiencing premature failure, but popular websites are more likely to endure. The early demise of these networks is linked to the rising quantities of child exploitation code words and photos, as well as the growing popularity of the website (Westlake and Bouchard 2016).

In a similar perspective, additional research demonstrates that the criminal process within Darkweb CSEM (Child Sexual Exploitation Material) groups encompasses several stages, actions, challenges, and individual and situational prerequisites, emphasizing the impact of the Darkweb on the modus operandi of criminal operations (Van Der Bruggen and Blokland 2022). Two factors that contribute to child exploitation networks on the Dark Web are the network structure and the communication over unlawful child pornography material (Fonhof et al. 2019).

Online anonymity, absence of parental oversight, and inadequate legal solutions are factors that enable and contribute to child sexual exploitation on the Internet (Caffo 2021). A separate study discovered a general decrease in the trafficking of child exploitation material on P2P networks from one month to another. It was determined that 9.5% of the apprehended traffickers had previously committed sexual offenses against minors in offline settings (Bissias et al. 2016).

Online child sexual exploitation material use is influenced by five unique factors: dissocial features, dysfunctional intimacy, passive alienation, normless alienation, and coping with the threat (Paquette et al. 2022). CSAM is highly prevalent in the Chinese dark web market and has been monetized, resulting in 3,449 sales during a 44-week monitoring period (Wang et al. 2023).

Psychological Impact of Exploitation on the Dark Web on Child Victims:

Many scholars show a severe psychological impact on victims of child exploitation on the dark web, including mental health effects, trauma, and long-term consequences for children who have been exploited online. Meanwhile, some studies suggest that exploitation on the dark web leads to severe psychological trauma, emotional degradation, and social maladjustment in child victims. The exploitation of children on the dark web is a severe issue with profound psychological impacts on the victims. This synthesis comprehensively consolidates various research papers' findings to understand these impacts.

Some scholars show that Children who are victims of trafficking and commercial sexual exploitation (CSE) experience significant physical and emotional trauma, including humiliation, violence, degradation, and unrelenting fear and abuse. According to Rafferty, Trafficking and CSE present grave risks to the physical, psychological, spiritual, and social-emotional development of young victims (Rafferty 2008). Furthermore, Victims of sex rings and pornography often show patterns of negative psychological and social adjustment, with those involved for more extended periods or in pornography experiencing more severe impacts. According to Burgess et al., Three-fourths of child victims exposed to sex rings and pornography demonstrated negative psychological and social adjustment (Burgess et al. 1984).

On the other hand, users of child sexual exploitation material (CSEM) often construct children online as less "real" and sexualized, which facilitates offending and helps them overcome psychological barriers. This detachment and normalization of abuse contribute to the ongoing victimization of children. According to Rimer, Online, CSEM users construct children differently, making them less or not "real" and sexualized, which facilitates offending and allows them to hold conventional beliefs about children and childhood while engaging in incongruent online activity (Rimer 2019).

Furthermore, prior sexual abuse significantly increases the risk of children being exploited, particularly among female youth. Physical and emotional abuse also contribute, though to a lesser extent, to the risk of sexual exploitation. According to Vries & Goggin, Sexual abuse considerably increases the risk of commercial sexual exploitation of youth, especially among female youth in the United States (Vries and Goggin 2020).

Moreover, dark web networks allow offenders to validate and normalize their actions, offering support and access to information and material. This environment perpetuates the cycle of abuse and exploitation. According to Kloess & Bruggen, Engagement in interpersonal communication and interactions with like-minded others in Dark Web networks serves validation, normalization, and support for child sexual exploitation and abuse users (Kloess and Bruggen 2023).

Meanwhile, some scholars show that Police teams investigating internet child exploitation may experience secondary traumatic stress due to the graphic images and sounds they are exposed to (Burns et al. 2008). Others see that Online child sexual exploitation and abuse (OCSEA) has predominantly social and psychological effects on children and youth despite being perceived as economically beneficial (Ramiro et al. 2019).

Furthermore, some scholars show that Severe exploitation of children in modern slavery and human trafficking exposes them to profound short-term and long-term physical, mental, psychological, developmental, and even generational risks to health (Wood 2020). Moreover, some see children and adolescents in posttrafficking care showed high symptom levels of depression, anxiety, and post-traumatic stress disorder, which are strongly associated with self-harm or suicidal behaviors (Kiss et al. 2015).

According to Vrubliauskaitė, Psychological factors like low self-esteem, dysfunctional attachment models, maladaptive problem-solving strategies, and post-traumatic stress disorder are linked to the risk of becoming a victim of commercial sexual exploitation (Vrubliauskaitė 2018).

In Conclusion, the psychological impact of exploitation on the dark web on child victims is profound and multifaceted. Victims suffer severe trauma, both physical and emotional, and often experience long-term adverse psychological and social adjustment. The normalization and detachment facilitated by dark web networks exacerbate these impacts, while prior abuse increases the risk of exploitation. Addressing these issues requires comprehensive prevention and rehabilitation strategies to mitigate the severe consequences for child victims.

Part Two—International and National Efforts to Control Dark Web Crimes Against Children:

There are a lot of international Interpol and Europol to control dark web crimes against children, besides other national efforts to comply with. One of these efforts was in May 2021, when law enforcement apprehended five German males, ranging in age from 40 to 64, who are believed to have operated "Boystown," a prominent online platform on the darknet dedicated to facilitating child sexual abuse (Connolly 2021).

As per the police, the online forum had been operational for two years and had amassed a membership of more than 400,000 registered users at its closure. Three apprehended individuals were charged with establishing and sustaining the online platform. In contrast, one individual was identified as one of the forum's most engaged participants, having substantially contributed to over 3500 postings. In 2015, a study discovered that there were 900 online forums dedicated to child sexual abuse, such as "Boystown," operating on the darknet. These sites collectively received an average of 168,152 daily inquiries (Owen and Savage 2015).

Several studies indicate that multinational endeavors, including collaboration through INTERPOL and Europol, legal frameworks, and training, are crucial, yet obstacles in legislation and execution are encountered. The rising occurrence of cybercrimes targeting children, including child pornography, internet grooming, and cyberbullying, has made it imperative to establish a worldwide response. Various international organizations and legislative frameworks have been established to address these issues.

This synthesis evaluates the efficacy of various global endeavors. International endeavors to address cybercrimes targeting children are crucial and have demonstrated efficacy through collaboration, legal harmonization, and preventive actions. Nevertheless, there are still obstacles to overcome, especially when it comes to ensuring the implementation of legislation and keeping up with the swift advancements in cybercrime methods. Uninterrupted global cooperation and method adjustment are essential to safeguarding youngsters in the era of digital technology.

Many researchers argue that combating cybercrimes against minors effectively necessitates solid international collaboration, as individual states possess limited capacities to address these crimes independently. International collaboration, facilitated by INTERPOL and Europol, is crucial in preventing, combating, and investigating cybercrimes targeting children (Calcara 2013).

Furthermore, it is widely recognized that international collaboration is vital in identifying and preventing cybercrimes targeting children to safeguard their well-being. This is in addition to the importance of appropriate domestic laws (Ivasyuk 2021). Furthermore, it is widely recognized that organizations such as INTERPOL and Europol have crucial responsibilities in coordinating global initiatives to prevent child pornography and other cybercrimes targeting children (Calcara 2013).

Several nations, especially in Latin America, have made significant progress in harmonizing their legislation with global norms to safeguard minors from online

exploitation. Nevertheless, there are still deficiencies in the legislation and enforcement. Latin American countries have found deficiencies in their laws and protocols for preventing and safeguarding minors who are victims of online sexual exploitation (Fernandes 2015).

However, some observers perceive that incorporating international and EU regulations into national legal systems, like Italy's, indicates advancement but also underscores persistent obstacles and crucial areas requiring enhancement. The Italian legal system encounters significant challenges in implementing the instruments adopted by international and EU legislation to combat cybercrimes against children (Russo and Parodi 2021).

Many people recognize the importance of implementing preventive measures such as education and social initiatives to combat cybercrimes targeting children. These endeavors receive backing from many international agreements and domestic initiatives to establish a more secure digital environment. Global initiatives to address cybercrimes targeting minors encompass the Convention on the Rights of the Child, the Penal Code, and the International Convention on Cybercrime (Nowicka and Zaroślak 2021).

However, some individuals recognize that the absence of borders in cybercrimes and the advancing technology employed by criminals provide substantial obstacles to conventional law enforcement techniques. Ongoing global training and collaboration are essential to tackle these concerns properly. International training is practical in tackling the severe worldwide issue of computer-facilitated crimes against children (Geldenhuys 2017).

Similarly, some scholars see the efficacy of the global legal system in addressing cybercrime as contingent upon elements such as national security, politics, economics, and public sentiment (Nukusheva et al. 2022). The text examines strategies to safeguard and educate youngsters regarding cyberbullying and cyberstalking in India, emphasizing the responsibility of the government and policymakers to prevent these offenses (Kumari 2021). According to a survey, there was a 15.5% increase in reported cybercrimes involving women and children in India between April and May 2017, despite implementing the World Plan for Women and Child Internet (Jadimath 2023). Mostly, children frequent social networking sites, and the primary online peril they face is sexual exploitation (Kahimise and Shava 2019).

Success Stories of Fostering International and National Efforts to Combat CSE on the Dark Web:

There are many success stories in arresting perpetrators of crimes of sexual exploitation of children via the Dark Web, in which Interpol and Europol participated in cooperation with law enforcement authorities in many countries. Among the most prominent of these stories are:

Arresting the Managers of a Dark web Platform for Publishing Images of Sexual Assault: The European Police Organization "Europol," in cooperation with both the German and American police, succeeded in arresting four Germans who ran a platform for publishing images of child sexual abuse on the dark web visited by nearly half

a million users, known as Boystown, in a multi-agency security operation with practical international security cooperation, with the participation of The German Federal Criminal Police, the Dutch Police, the Swedish Police, the Australian Anti-Child Exploitation Centre, the Australian Federal Police, the Queensland Police Service, the US Federal Bureau of Investigation, US Immigration and Customs Enforcement, and the Royal Canadian Mounted Police.

This international security operation began with an investigation by the German Federal Criminal Police Office into one of the most widespread child sexual abuse platforms in Europe on the dark web, where arrests of suspects were made in Germany (3) and Paraguay (1), and the detainees had roles. The dark web platform was removed by an international task force set up by the German Federal Criminal Police, which included Europol and law enforcement agencies from the Netherlands, Sweden, Australia, Canada, and the United States. This site focused on child sexual abuse. It had 400,000 registered users when it was removed.

On the same occasion, several other dark web chat sites used by children who committed sexual crimes were also seized. Online communities of child offenders on the dark web (as Europol finds) show great flexibility in responding to law enforcement actions targeting them. Their responses include reviving old communities, creating new ones, and making solid efforts to organize and manage them. Images and video data seized during this investigation have been used for victim identification task forces regularly organized at Europol. Further arrests and rescues are expected globally. Police worldwide are examining intelligence packages from Europol (El-Kady 2024).

Arresting a Pedophile in the Dark Web: Some press reports indicate that the dark web contributed to the rescue of a seven-year-old Russian child from the clutches of a pedophile, who kidnapped him and held him in an underground bunker for 52 days in Russia. The process of freeing the child was carried out with the intervention of Russian special forces. In cooperation with Interpol, information related to the child was received through Interpol channels of the Russian police, as the child's presence became known from publications on the dark internet.

Dismantling a Child Exploitation Network in the Dark Web: Interpol's efforts resulted in the dismantling of an international child sexual exploitation network on May 23, 2019, which was communicating via the dark web, in an operation that resulted in the arrest of 9 people in three countries. Interpol launched this operation in 2017 following the discovery of materials showing the sexual exploitation of children. On a website on the Dark Web, which includes about 63,000 members, this operation allowed the rescue of 50 children. Following a request from Interpol, investigators from several countries analyzed the published materials and identified electronic addresses (IP) in Thailand, Australia, and the United States.

Bulgaria's Anti-Cybercrime Authority turned off the website, which had been publishing new material weekly for several years. Among the nine suspects arrested, the leading operator of the website was identified as a man residing in Thailand who was accused of committing sexual abuse against 11 children. Among them is one of his relatives, and one of the other operators of this website was arrested in

Australia. Thousands of documents were found in his possession showing sexual violations against children who were photographed in Thailand and Australia. These photos showed that he was the main responsible for violations against children, one of whom was no more than 15 months old, while One of the two men was sentenced to 146 years in prison and the other 40 years in jail in their respective countries (El-Kady 2024).

Legal Challenges in Combating CSE on the Dark Web:

Due to its anonymous nature and the rapid evolution of technology, the dark web presents significant challenges for law enforcement agencies (LEAs) in combating child exploitation. This synthesis explores the critical legal and investigative challenges identified in recent research. Many studies suggest that combating child exploitation on the Dark Web faces significant legal challenges due to inconsistent international legislation, rapid technological advances, and the need for coordinated efforts between law enforcement, industrial, and non-governmental organizations.

Some studies see that the lack of consistent international definitions and legislative frameworks creates opportunities for child exploitation, highlighting the need for clear national and international definitions. According to Hillman et al., clear national and international definitions are needed to combat online child exploitation, as a lack of consistency in the international legislative environment creates opportunities for sexual exploitation (Hillman et al. 2014). Meanwhile, others add that the Lack of direct governance by an international body compounds the problem of child exploitation on the Dark Web (Kierkegaard 2008).

On the other hand, some studies show that Rapid technological advances complicate the investigation of child exploitation material (CEM) by increasing the scope of spaces to police and the complexity of these environments. According to Holt et al., challenges in investigating online child exploitation material offenses include the scope of the problem, rapid technological advances, and the need for engagement from industrial and non-governmental organizations (Holt et al. 2020).

Meanwhile, others see that the dark web's anonymity and the need for specialized techniques, such as Open-Source Intelligence (OSINT), pose significant challenges for LEAs in identifying and prosecuting offenders. Rajamäki sees that the biggest challenges faced by law enforcement agencies in combating child exploitation on the Dark Web are related to data storage and the criminal investigation itself (Rajamäki et al. 2022).

In the same context, some scholars see that existing legislative and prosecution-based approaches are insufficient, necessitating a multifaceted approach that includes non-prosecutorial strategies and collaboration with industrial and non-governmental organizations (Hillman et al. 2014; Holt et al. 2020). According to Quayle, changing the environments that support online child exploitation and abuse is necessary to detect, manage, and prevent these crimes (Quayle 2020).

On the other hand, some see that offenders on the dark web develop trust and relationships through online networks, which validate and normalize their activities, making it harder for LEAs to infiltrate these networks. According to Kloess & Bruggen, Trust and relationship development among users in Dark Web child sexual

exploitation networks is crucial for validation, normalization, and support, as well as access to expert advice and information (Kloess and Bruggen 2023).

Meanwhile, others see proactive strategies, such as those employed by Queensland Police's Taskforce Argos, which involve covert infiltration and the ability to commit controlled criminal acts, as having succeeded despite evidence-collection concerns. According to Bleakley, Taskforce Argos has been successful in infiltrating online forums dedicated to child exploitation material despite concerns regarding evidence collection (Bleakley 2019).

Lastly, some see that effective combat against online child exploitation requires international cross-disciplinary collaboration to identify, locate, and safeguard victims, as well as to prevent, investigate, and prosecute these crimes (Quayle 2020; Kierkegaard 2008).

In conclusion, combating child exploitation on the dark web requires overcoming significant legal and technological challenges. Inconsistent international legislation, the rapid evolution of technology, and the need for specialized investigative techniques complicate efforts. A multi-faceted approach that includes legislative reform, proactive law enforcement strategies, and international collaboration is essential to address this issue effectively.

International Legal and Policy Challenges:

The prosecution and investigation of child sexual exploitation, particularly online, face significant challenges due to varying international legal frameworks and policy gaps. This synthesis explores these challenges and the role of international treaties like the Budapest Convention on Cybercrime. Many studies suggest that challenges in international cooperation, differing legal frameworks, and policy gaps that hinder effective prosecution and investigation of child sexual exploitation include insufficient interaction between law enforcement agencies, jurisdictional issues, and inconsistent legislative environments, while existing international treaties like the Budapest Convention play a crucial role in addressing these issues.

Some scholars show that many countries have weak domestic laws that are insufficient to combat cyber offenses effectively. The borderless nature of cyberspace complicates jurisdiction, making it difficult to investigate and prosecute cybercrimes. Some see that the Budapest Treaty is the best international legal framework to fight cybercrimes and needs the comity of nations to ally with (Ali et al. 2022). Clear national and international definitions are needed to address online child exploitation, as a lack of consistency in the international legislative environment creates opportunities for sexual exploitation (Hillman et al. 2014).

Furthermore, insufficient interaction between law enforcement agencies in different countries and the lack of an agreed mechanism for obtaining external data hinder effective prosecution. Multilateral and bilateral agreements are often not well-organized, leading to gaps in cooperation. Some see that close ties at the international law enforcement systems level can effectively overcome challenges like insufficient interaction between law enforcement agencies and lack of an agreed mechanism for obtaining external data (Macidov 2023).

Moreover, others see that barriers to practical cooperation in child sex tourism cases include the admissibility of foreign evidence, involvement of non-police organizations in police operations, and lengthy diplomatic processes. These barriers impede practical cooperation. Interagency cooperation and collaboration among foreign police are crucial but often lacking (De Vries 2021). In the same context, some see that the lack of consistency in international legislative definitions creates opportunities for the sexual exploitation of children. Clear national and international definitions are necessary to address these crimes effectively (Hillman et al. 2014).

Regarding the role of international treaties and agreements, scholars agreed that the Budapest Convention on Cybercrime is highlighted as a significant international legal framework for combating cybercrimes. It benefits member states and is considered the best treaty for fighting cybercrimes, necessitating global cooperation (oglu Macidov 2023; Ali et al. 2022).

In conclusion, the effective prosecution and investigation of child sexual exploitation are hindered by inadequate domestic laws, jurisdictional challenges, and insufficient international cooperation. The lack of clear and consistent international legislative definitions further complicates efforts. However, international treaties like the Budapest Convention on Cybercrime are crucial in providing a framework for cooperation and combating these crimes. Enhanced interagency cooperation, streamlined diplomatic processes, and consistent legislative definitions are essential to overcoming these challenges.

Part Three- Cutting-edge Technologies in Detecting CSE on the Dark Web:

The detection of child exploitation on the dark web is a critical and challenging task that has seen significant advancements through the application of various cutting-edge technologies. These technologies aim to identify and mitigate the spread of child exploitation material by leveraging advanced data analysis, machine learning, and artificial intelligence. Studies suggest cutting-edge technologies for detecting child exploitation on the dark web include deep convolutional neural networks (CNNs), OSINT automation tools, AI-powered speech recognition and keyword spotting, and intelligent software-agent systems.

Deep convolutional neural networks (CNNs) are used to detect child pornography content in images by leveraging transfer-learning strategies. These networks are trained on large datasets and fine-tuned for specific detection tasks, outperforming existing solutions. According to Vitorino et al., deep convolutional neural networks (CNNs) are effective in detecting child pornography content in images, outperforming existing solutions (Vitorino et al. 2018).

Law Enforcement Agencies (LEAs) utilize OSINT automation tools to investigate child abuse material on the dark web. These tools help identify darknet sites used by criminals while addressing challenges related to data storage and the legality of handling such sensitive content. According to Rajamäki, OSINT automation tools can be exploited on the Dark Web to find darknet sites used by criminals, addressing challenges related to data storage and criminal investigation (Rajamäki et al. 2022).

AI-powered speech recognition systems, such as Wav2vec2.0 and Whisper, are employed to transcribe and analyze audio data for keywords related to child abuse.

These systems achieve high accuracy rates and use federated learning to maintain data privacy while improving performance. According to Vásquez-Correa & Muniain, Speech recognition and keyword spotting using Wav2vec2.0 and Whisper models can detect child abuse keywords with true-positive rates between 82 and 98% (Vásquez-Correa and Álvarez Muniain 2023).

Intelligent agents are developed to locate missing and exploited children by performing knowledge discovery, predictive data mining, and intelligent search and discovery on the internet and intranets. These agents assist in ongoing and future investigations by automating the search and analysis processes. According to Romaniuk, Analytic Services is developing an intelligent software-agent system to locate missing and exploited children using knowledge discovery and predictive data mining (Romaniuk 2000).

In conclusion, several advanced technologies are bolstering the fight against child exploitation on the dark web. Deep neural networks are proving effective in image detection, while OSINT tools and intelligent software agents enhance the capabilities of law enforcement agencies. Additionally, AI-powered speech recognition systems offer promising solutions for analyzing audio data. Together, these technologies represent significant strides in detecting and combating child exploitation online.

AI-driven Detection Tools in Combating CSE on the Dark Web:

The rise of child exploitation material on the dark web presents a significant challenge for law enforcement agencies (LEAs). AI-driven detection tools have emerged as a critical component in combating this issue, offering advanced capabilities in identifying and analyzing such content. Based on recent research findings, this synthesis explores the role of AI-driven detection tools in addressing child exploitation on the dark web. Studies suggest that AI-driven detection tools play a crucial role in combating child exploitation on the dark web by transcribing and analyzing audiovisual data, detecting keywords related to child abuse, and identifying children's faces in images.

AI-powered speech recognition systems like Wav2vec2.0 and Whisper can transcribe audiovisual data and detect keywords related to child abuse with high accuracy. These systems achieve a word error rate between 11 and 25% and true-positive rates between 82 and 98% for keyword spotting, depending on the language. Federated learning enhances the performance of these AI systems while maintaining data privacy, making them more robust for forensic applications in child abuse cases. According to Vásquez-Correa & Muniain, AI-driven detection tools, like speech recognition and keyword spotting, help detect evidence of child abuse in audio data and provide a more robust platform for forensic applications (Vásquez-Correa and Álvarez Muniain 2023).

On the other hand, Deep learning methodologies can automatically identify children's faces in images previously labeled as pornographic, aiding LEAs in tracking online child abuse and related crimes. These systems learn features directly from training images, achieving high precision, recall, and overall accuracy in recognizing child faces. According to Islam et al., AI-driven detection tools help track

online child abuse, bullying, and sexual assault and detect cybercriminals targeting children for molestation later (Islam et al. 2019).

In conclusion, AI-driven detection tools play a crucial role in combating child exploitation on the dark web. Speech recognition systems and deep learning methodologies significantly enhance the ability of law enforcement agencies to identify and analyze child exploitation material. These tools not only improve detection accuracy but also ensure data privacy through federated learning, making them indispensable in the fight against online child abuse.

Ethical Considerations of Using AI and Digital Tools in Combating CSE on the Dark Web:

The use of artificial intelligence (AI) to combat child exploitation on the Dark Web presents significant ethical considerations. These considerations are crucial as they involve vulnerable populations and high-stakes environments. The following synthesis highlights the critical ethical concerns identified in the research literature. Studies suggest that the ethical considerations of using AI to combat child exploitation on the Dark Web include addressing bias in datasets, privacy risks, potential misuse, and the need for transparent ethics disclosures.

Scholars see that AI systems can perpetuate and amplify biases present in the datasets used for training, which can disproportionately affect already vulnerable populations. The collection and reporting of data necessary for AI can pose significant privacy risks to individuals, including victims and users of the Dark Web. There is a risk that AI tools designed to combat child exploitation could be misused, either by authorities or malicious actors, leading to unintended harm.

In addition, engaging a broader range of stakeholders, including survivors and diverse populations, in designing AI systems can help mitigate some ethical risks and ensure the tools are more effective and equitable. Researchers and developers should include transparent ethics disclosures to ensure accountability and public trust in AI applications. According to Deeb-Swihart et al., Ethical tensions in AI-based combating of human trafficking include bias in datasets, privacy risks, and potential misuse (Deeb-Swihart et al. 2022).

Additionally, the dynamics of trust and relationships among users of dark web networks are complex and high-risk, and AI systems must navigate carefully to avoid exacerbating these risks. According to Kloess & Bruggen, interpersonal communication and interactions with like-minded others in Dark Web networks serve various functions, including validation, normalization, and support (Kloess and Bruggen 2023).

Technological Solutions Beyond AI and Its Role in Combating CSE on the Dark Web:

The rise of blockchain technologies, cryptocurrencies, and advanced digital forensics has significantly impacted the landscape of dark web investigations. These technological solutions offer new methods for secure evidence preservation, tracking illicit payments, and enhancing digital forensic capabilities. Studies suggest that

blockchain technologies enhance secure evidence preservation, cryptocurrency analysis aids in tracking illegal payments, and advanced digital forensics improve dark web investigations by ensuring traceability, privacy, and integrity of digital evidence.

Blockchain for Secure Evidence Preservation:

Scholars see that Blockchain's decentralized and tamper-resistant nature ensures the integrity and validity of digital evidence, making it difficult to alter or hack stored information. Some suggest that the block-DEF framework uses blockchain technology to securely store and retrieve evidence, balancing privacy and traceability (Tian et al. 2019). Others see that Blockchain technologies can make crime evidence preservation more secure and transparent while enhancing digital forensics and cryptocurrency analysis in dark web investigations (Shetty et al. 2023). In addition, some see that Blockchain technologies can provide proof of existence and privacy preservation for examining evidence items in digital forensics investigations, increasing trust between evidential entities and examiners (Li et al. 2019).

In the same context, some consider that frameworks like Block-DEF and IoT forensic chain (IoTFC) provide scalable solutions for maintaining evidence information separately from the evidence itself, balancing privacy and traceability (Tian et al. 2019; Li et al. 2019). They see that Blockchain can enhance transparency and security in digital forensics by storing forensic data in a peer-to-peer network, ensuring that evidence remains unaltered and accessible across jurisdictional borders (Shetty et al. 2023; Li et al. 2019).

Cryptocurrency Analysis for Tracking Illicit Payments:

Scholars see that Cryptocurrencies, particularly Bitcoin, are commonly used for illegal transactions on the dark web due to their perceived anonymity. However, blockchain technology allows for the tracking and analysis of these transactions. According to Dyson, Blockchain technologies can create new areas of investigation and help track payments related to illegal activities. However, more research is needed to understand digital forensics and data retention in the blockchain era (Dyson 2019). Furthermore, Dearden and Tucker estimate that Cryptocurrency transactions on the darknet are generally identifiable (90%) and involve likely illegal transactions. These transactions attempt to obfuscate other legal transactions (Dearden and Tucker 2023).

Moreover, others see that Blockchain technologies can improve law enforcement by preventing and technologically blocking illegal operations with cryptocurrencies, aiding in investigating criminal offenses committed in cyberspace (Kalaida 2021).

In the same context, some scholars have investigated darknet marketplaces like AlphaBay and shown that cryptocurrency transactions can be identified and analyzed to uncover illegal activities and patterns (Dearden and Tucker 2023). Others show that Cryptomixing services, which launder payments to evade detection, pose challenges for investigators but also highlight the need for advanced analytical tools to track and disrupt these services. According to Holt et al., Cryptomixing services, payments are effectively laundered to circumvent detection and investigation tools, facilitating illicit online transactions (Holt et al. 2023).

Advanced Digital Forensics in Dark Web Investigations:

Scholars see that digital forensics tools are evolving to handle the complexities of Web3 wallets and other blockchain-based applications, enabling investigators to recover and analyze digital evidence from mobile devices. These tools help investigators unlock the full potential of popular cryptocurrency Web3 wallets, Trust Wallet, and Metamask and recover artifacts related to illegal activities on Android and iOS devices (Mirza et al. 2022).

In addition, Using smart contracts and decentralized anonymous credentials in blockchain-based forensic frameworks ensures fine-grained access control and privacy preservation while maintaining evidence accountability. For example, some scholars examine Eunomia, an anonymous and secure vehicular digital forensics scheme based on blockchain, which preserves privacy and ensures access control and traceability (Li et al. 2023).

On the other hand, scholars see that integrating blockchain with digital forensics enhances the ability to trace and verify the provenance of evidence, providing a robust audit trail that increases trust in the investigation process (Li et al. 2023; Li et al. 2019).

In conclusion, Blockchain technologies, cryptocurrency analysis, and advanced digital forensics collectively enhance the capabilities of dark web investigations. Blockchain ensures secure and tamper-proof evidence preservation, while cryptocurrency analysis enables the tracking of illicit payments. Advanced digital forensics tools further support these efforts by providing detailed insights and maintaining the integrity of digital evidence. Together, these technologies offer a comprehensive approach to tackling illegal activities on the dark web.

Part Four- Preventive Strategies in Combating CSE on the Dark Web:

Child exploitation on the Dark Web is a significant and growing concern, necessitating the development of effective preventive strategies. Various research papers have explored different approaches to combat this issue, ranging from law enforcement tactics to psychological interventions and public health strategies. Some studies suggest that preventive strategies in combating child exploitation on the Dark Web include proactive law enforcement operations, online warning messages, therapeutic interventions for at-risk individuals, and international collaboration.

Some scholars show that. Taskforce Argos has successfully infiltrated Dark Web child exploitation networks by adopting proactive strategies and operating with relatively loose restrictions, allowing officers to commit controlled undercover operations. According to Bleakley, Taskforce Argos, a Queensland Police unit, has been successful in covertly infiltrating online forums dedicated to child exploitation material despite concerns about evidence collection (Bleakley 2019).

Meanwhile, others see that offenders on the Dark Web develop trust and relationships through interpersonal communication, which validates and normalizes their activities. This trust is crucial for their operations but also represents a vulnerability that can be exploited by law enforcement. According to Kloess & Bruggen, engagement in interpersonal communication and interactions with like-minded others in

Dark Web networks serves validation, normalization, support, and access to expert advice and information (Kloess and Bruggen 2023).

In the same context, other scholars give an example of the German Dunkelfeld Project that focuses on individuals at risk of committing sexual offenses against children, offering preventive assessment and treatment. This approach targets those who admit to having a sexual interest in children, aiming to prevent offenses before they occur. According to Beier, Proactive strategies include research on individuals at risk of committing first or persistent sexual offenses against children and offering preventive assessment and treatment (Beier 2016a, 2016b). He proves that The German Dunkelfeld approach reduces risk factors for child sexual abuse, prevents sexual offending against minors, and reduces the number of contact offenses and child pornography offenses (Beier 2016a, 2016b).

Otherwise, some see that online warning messages can effectively dissuade individuals from accessing child sexual exploitation material (CSEM). Messages that highlight the ability of police to track IP addresses and the potential illegality of the content are particularly effective. According to Prichard et al., warning messages advising of potential harm to viewers, victims, or police tracking IP addresses can effectively reduce access to online child sexual exploitation material (Prichard et al. 2022).

Furthermore, some scholars show that digital media interventions, such as search engine advertisements, can redirect potential CSEM users to therapeutic services. Effective advertisements are designed based on insights into the mindset and barriers faced by these individuals. According to Henry, Effective digital advertisements can divert potential users away from child sexual exploitation material and encourage them to reach out to a helpline (Henry 2020).

On the other hand, some emphasize that international collaboration is essential for identifying, locating, and safeguarding victims, as well as for preventing and prosecuting online child exploitation and abuse. Changing the environments that support these crimes is necessary for effective prevention. According to Quayle, changing the environments that support online child exploitation and abuse is necessary to detect, manage, and prevent these crimes (Quayle 2020).

Additionally, some show that applying social learning theory to online child sexual abuse behavior suggests that prevention efforts should involve family, school, community, and social values to reduce juvenile delinquency on the Dark Web. According to Yang et al., an innovative social learning strategy to battle online child sexual abuse is proposed to reduce juvenile delinquency on the dark web (Yang et al. 2021).

Lastly, others suggest a comprehensive approach to child safety online, including addressing risks associated with digital technology, such as day-care and school journaling apps, online gaming, social media, and messaging apps. According to Pendergast, Proactive approaches to child safety online, focusing on day-care and school journaling apps, online gaming, social media, and messaging apps, can help combat child exploitation (Pendergast 2023).

In conclusion, preventing child exploitation on the Dark Web requires a multifaceted approach. Effective strategies include proactive law enforcement operations,

preventive assessment and treatment programs, automated warning messages, and digital advertisements. Additionally, international collaboration and the application of social learning theory are crucial for creating safer online environments. By combining these strategies, it is possible to reduce the incidence of child exploitation and protect vulnerable children from harm.

Coping Strategies Employed by Child Victims of Dark Web Exploitation:

Some studies suggest that child victims of dark web exploitation employ coping strategies such as seeking validation, normalization, and support through interpersonal communication and interactions with like-minded individuals. The exploitation of children on the dark web is a severe and complex issue involving various psychological and criminological dimensions. Understanding the coping strategies employed by child victims is crucial for developing effective support mechanisms and interventions.

Victims often communicate and interact with like-minded individuals, serving functions such as validation, normalization, and support. This engagement helps them cope with dark web networks' high-stakes and risky environment. Establishing and maintaining trust within dark web networks is crucial for victims. This trust helps them navigate the continuous flow of threats and manage the demands and commitments of these environments.

According to Kloess & Bruggen, Engagement in interpersonal communication and interactions with like-minded others in Dark Web networks serves validation, normalization, and support for child victims of sexual exploitation and abuse (Kloess and Bruggen 2023).

In conclusion, child victims of dark web exploitation employ coping strategies that primarily revolve around interpersonal communication and the development of trust within their networks. These strategies provide them with validation, normalization, and support, essential for managing dark web environments' high-stakes and risky nature. Understanding these coping mechanisms is vital for creating effective support systems and interventions for these vulnerable individuals.

Coping Strategies for Law Enforcement Dealing with Internet Child Exploitation:

Some studies suggest that law enforcement coping strategies for dealing with internet child exploitation include organizational support, personal coping mechanisms, and procedural safeguards. Investigating Internet Child Exploitation (ICE) is a highly stressful and emotionally taxing task for law enforcement officers. This synthesis explores the coping strategies these officers employ to manage the psychological and emotional challenges associated with their work.

Some scholars show that organizational support, such as access to mental health services, peer support programs, and structured debriefing sessions, often facilitates effective coping. According to Powell et al., ICE investigators use individual and organizational coping resources to cope with the stress of investigating internet child exploitation (Powell et al. 2014).

Meanwhile, Burns et al. show that organizational and personal strategies can assist police teams investigating internet child exploitation to cope more effectively (Burns et al. 2008). Moreover, Krause et al. see that law enforcement personnel involved in internet child exploitation investigations face unique stresses and stress reactions, which can be mitigated through procedural safeguards and model programs (Krause et al. 2009).

On the other hand, Specialized task forces, such as the Internet Crimes Against Children (ICAC) Task Force, provide a structured environment and resources that help officers manage stress and improve productivity. According to Marcum & Higgins, Successful ICAC task forces depend on specialized training, practical investigation, and strong collaboration between federal, state, and local law enforcement agencies (Marcum and Higgins 2011).

Furthermore, some show that officers employ personal coping strategies such as compartmentalization, maintaining a solid work-life balance, and engaging in physical activities to manage stress (Powell et al. 2014; Burns et al. 2008). According to Seigfried-Spellar, Individuals working as both digital forensic examiners and investigators of child pornography cases reported higher secondary traumatic stress, feelings of worthlessness, and lower concentration (Seigfried-Spellar 2018). Additionally, developing a sense of purpose and focusing on the positive outcomes of their work, such as rescuing children, helps officers cope with the emotional toll (Burns et al. 2008; Krause et al. 2009).

On the other hand, some see that selecting ideal applicants who are psychologically resilient and providing them with specialized training on coping mechanisms can mitigate the impact of stress (Powell et al. 2014). Continuous professional development and training in stress management techniques are also crucial for maintaining the well-being of ICE investigators (Krause et al. 2009).

Moreover, others see that Strong peer support and team cohesion are vital for coping with the emotional impact of ICE investigations. Sharing experiences and supporting each other helps reduce feelings of isolation and stress. In addition, Critical Incident Stress Debriefing (CISD) and peer support programs effectively provide emotional support and reduce secondary traumatic stress (Burns et al. 2008; Krause et al. 2009).

Lastly, according to Krause et al., officers dealing with ICE cases need Access to mental health services and counseling. Encouraging the use of these services can help manage stress and prevent burnout (Krause et al. 2009). Meanwhile, according to Seigfried-Spellar, Officers who perform both investigative and digital forensic duties are at higher risk for psychological distress and may benefit more from targeted mental health interventions (Seigfried-Spellar 2018).

In Conclusion, Law enforcement officers dealing with Internet Child Exploitation employ a combination of organizational support, personal coping mechanisms, peer support, and access to mental health services to manage the significant stress associated with their work. Effective coping strategies include structured organizational resources, personal resilience, strong team cohesion, and continuous training. These strategies collectively help officers maintain their psychological well-being and continue their critical work in combating child exploitation online.

Preventive Measures and Educational Campaigns for CSE on the Dark Web:

Child sexual exploitation (CSE) is a pervasive issue that necessitates comprehensive preventive measures and educational campaigns. Various strategies have been implemented globally, focusing on public awareness, educational programs for different stakeholders, and policy-driven efforts. This synthesis highlights the key insights from multiple research papers on effective preventive measures and educational campaigns against CSE.

Many studies suggest that school-based educational programs, public awareness campaigns, and policy-driven preventive efforts can increase knowledge and self-protective behaviors in children. However, their impact on the actual reduction of child sexual abuse remains inconclusive.

School-Based Educational Programs:

Some scholars see that School-based programs significantly improve children's knowledge about CSE and self-protective behaviors. These programs often teach children to identify dangerous situations, resist inappropriate touching, and seek help. Zwi et al. show that school-based child sexual exploitation intervention programs significantly improve knowledge measures and protective behaviors (Zwi et al. 2007). In the same context, Walsh et al. see that school-based education programs can increase children's self-protective skills and knowledge, but it is unknown if these gains decrease the likelihood of child sexual abuse (Walsh et al. 2018).

Furthermore, others see that School-based CSE prevention programs use educational content delivered through films, plays, discussion, and role-play with the most success (Fryda and Hulme 2015). Others see that school-based educational programs teach children skills to identify dangerous situations and promote disclosure, but studies are inconclusive about reducing victimization (Finkelhor 2009).

On the other hand, research shows that children as young as three can effectively learn self-protection skills through successful programs that involve significant parental and family participation (Kenny et al. 2008). These programs have successfully enhanced children's self-protective skills and knowledge retention. However, their impact on reducing CSE incidents remains inconclusive (Zwi et al. 2007; Walsh et al. 2018; Fryda and Hulme 2015; Finkelhor 2009). Effective delivery methods, such as films, plays, discussions, and role-playing, with repeated exposure, have been shown to help maintain knowledge gains (Fryda and Hulme 2015; Kenny et al. 2008).

Parental and Family Involvement:

Research indicates that involving parents and families in educational programs significantly enhances the effectiveness of CSA prevention efforts. Programs that include components directed at parents and family members reinforce the messages taught to children and provide a supportive environment for disclosure and prevention (Kenny et al. 2008). In a similar vein, a broad-based media campaign targeting adults, a one-to-one communications strategy, and a systems change strategy were used in

the evaluation of a child sexual abuse prevention program in Vermont (Chasan-Taber and Tabachnick 1999).

Policy-Driven Preventive Efforts:

Some studies focus on offender management strategies, such as registering sex offenders, community notification, and background checks, which are widely implemented but have limited evidence of effectiveness in preventing CSE. These strategies often focus on a stereotyped view of offenders and may not address the broader spectrum of abusers.

In the same context, others see that broader government-led or community-wide interventions are needed to address the prevalence of CSE and improve safety conditions in various contexts. Evaluations of such interventions are necessary to determine their efficacy (Finkelhor 2009). Furthermore, others see that most interventions in developing countries focus on preschool and primary school-aged children, with little focus on population-level interventions (Russell et al. 2020).

Public Awareness Campaigns:

Some studies focus on media and social media campaigns successfully reaching large audiences. These campaigns raise awareness about CSE and encourage help-seeking behaviors among potential offenders and victims. These campaigns can reduce risk factors and enhance protective factors against CSE. According to Ryckman et al., education and awareness campaigns can prevent abuse before it happens and help victims come forward for support and retribution (Ryckman et al. 2020). Furthermore, some show that Prevention initiatives like helplines, treatment, psychoeducation, online self-management courses, education, and awareness campaigns can encourage help-seeking and reduce risk factors for child sexual abuse material offending (Gannoni et al. 2023).

In the same context, others see that public health campaigns targeting adults, including broad-based media efforts and one-to-one communication strategies, have shown promise in increasing awareness and knowledge about CSE. However, their direct impact on prevention requires further evaluation (Chasan-Taber and Tabachnick 1999).

Online Safety Education:

Some academics see that education and awareness campaigns explicitly targeting online sexual abuse of children are crucial. These programs aim to prevent abuse before it happens and help victims come forward to seek support and retribution. (Ryckman et al. 2020).

In conclusion, preventive measures and educational campaigns against child sexual abuse are multifaceted, involving school-based programs, parental involvement, policy-driven efforts, and public awareness campaigns. School-based programs effectively increase knowledge and self-protective behaviors among children, while parental involvement enhances these efforts. Policy-driven strategies and public awareness campaigns are crucial in creating a supportive environment for prevention and disclosure. However, further research and comprehensive evaluations are

needed to determine the long-term effectiveness of these interventions in reducing the prevalence of CSE.

Proactive Prevention Strategies to Combat CSE:

The increasing prevalence of digital technology has brought about significant risks for children, including child sexual exploitation (CSE). Proactive prevention strategies are essential to mitigate these risks and ensure a safer digital environment for children. These strategies include digital literacy programs, educational campaigns, and the role of policymakers in creating a safer online space. Many studies suggest proactive prevention strategies to combat CSE, including digital literacy programs, educational campaigns, and the involvement of policymakers in creating a safer digital environment.

Digital Literacy Programs:

Some academics focus on digital literacy education as crucial for equipping children and teenagers with the skills to navigate the online world safely. Programs should integrate digital literacy, critical thinking, and responsible online behavior to foster a safer digital environment. According to Voicu & Crăciun, Preventive online safety education for teenagers integrates digital literacy, critical thinking, and responsible online behavior, fostering a safer digital environment (Voicu and Crăciun 2023). In the same context, others see that a critical digital literacy approach allows students to explore and discuss controversial issues within a supportive environment, helping develop appropriate skills to engage with the Internet as it is (McNicol 2016).

Meanwhile, others see the need for parents and teachers to collaborate to facilitate digital literacy education, provide proper guidelines for online activities, and help children become more productive users in the digital era. Some see that maintaining a regulatory approach, establishing special agencies, and facilitating digital literacy education are necessary to minimize the four significant online risks for children and youth (Jang and Ko 2023).

Educational Campaigns:

Some emphasize that education and awareness campaigns are effective methods to prevent online child sexual exploitation before it occurs and to assist victims in coming forward to seek support and retribution. These campaigns should target children, adolescents, and their guardians. (Ryckman et al. 2020). In addition, others consider public awareness and education strategies, such as those pursued under the EU's Safer Internet Programme, to play a significant role in enhancing the safety of children online by transforming child safety issues into legal and social obligations. According to Savrimuthu, the EU enhances the safety of children in the online environment through public awareness and education strategies, such as the Safer Internet Programme (Savirimuthu 2011).

Role of Policymakers:

Some academics show that a regulatory approach to the online exposure of children under 13 is necessary. Policymakers should establish special agencies in charge

of online safety for children and youth, encompassing all relevant stakeholders, including educators and digital firms. Multilateral discussions within international bodies like the OECD and UN subsidiaries should continue to lead international cooperation on online child safety (Jang and Ko 2023).

In the same context, some suggest that continuous assessment and adaptation of government strategies are essential to address the evolving threat landscape. This includes enhancing policy frameworks, improving international cooperation, investing in education and awareness, and fostering public–private partnerships. According to Moses, enhancing a strong policy framework, improving international cooperation, investing in education and awareness, and fostering public–private partnerships are recommended to improve the Nigerian Government's child online protection strategies (Moses 2023).

In conclusion, proactive prevention strategies to combat CSE involve a multifaceted approach that includes digital literacy programs, educational campaigns, and robust policymaking. Digital literacy education equips children with the necessary skills to navigate the online world safely while educational campaigns raise awareness and support victims. Policymakers are crucial in establishing regulatory frameworks and fostering international cooperation to create a safer digital environment for children. Collaboration among educators, parents, policymakers, and digital firms is essential to ensure comprehensive online safety for the next generation.

5 Conclusion

The chapter concluded that criminals use the dark web to commit severe crimes against children, such as Child trafficking and child abuse, taking advantage of the characteristics of this dark network, the most prominent of which is anonymity and the difficulty of tracking the perpetrators of crimes on this network. Research shows that exposure to criminal activities on the dark web can lead to psychological issues like secondary traumatic stress, reduced well-being, anxiety, self-esteem, and social competence in children, especially those involved in child exploitation. The normalization and validation of such actions in dark web networks exacerbate these issues.

The chapter emphasized the imperative of coordinated international initiatives and the enhancement of global security and judicial collaboration to combat illegal activities targeting minors via the dark web effectively. We must enhance security coordination for information exchange and address criminal activities perpetrated on the dark web while also broadening the establishment of bilateral and multilateral security agreements to combat cybercriminal activities online, particularly on the dark web.

Furthermore, to facilitate effective confrontation, contemplate establishing specialized security units to address dark web offenses, enhancing Interpol's capacity to coordinate these units, and providing law enforcement agencies with the requisite technical assistance and advanced training to investigate crimes associated with the

hidden network, particularly those targeting children perpetrated through the dark web. We must persist in advancing technical solutions to monitor and detect crimes against children perpetrated on the dark web, including information mining tools, network crawlers for data indexing, analytical tools for tracing encrypted virtual currency transactions, and blockchain software for preserving digital evidence.

References

Ali, A., Khan, I., & Bashir, S. (2022). NEED OF INTERNATIONAL LEGISLATION REGARDING CYBER CRIMES: PAKISTAN PERSPECTIVE. *Pakistan Journal of Social Research*, *4*(2), 1136–1144.

Audrin, C., & Blaya, C. (2020). Psychological well-being in a connected world: The impact of cybervictimization in children's and young people's life in France. *Frontiers in psychology*, *11*, 1427.

Beier, K. M. (2016a). Proactive strategies to prevent child sexual abuse and the use of child abuse images: Experiences from the German Dunkelfeld project. *Women and Children as Victims and Offenders: Background, Prevention, Reintegration: Suggestions for Succeeding Generations (Volume 2)*, 499–524.

Beier, K. M. (2016b). Proactive strategies to prevent child sexual abuse and the use of child abuse images: The German Dunkelfeld-Project for Adults (PPD) and Juveniles (PPJ). *Sexual violence: Evidence based policy and prevention*, 249–272.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child abuse & neglect*, *52*, 185–199.

Bleakley, P. (2019). Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks. *The Police Journal*, *92*(3), 221–236.

Bourke, M. L., & Craun, S. W. (2014). Secondary traumatic stress among internet crimes against children task force personnel: Impact, risk factors, and coping strategies. *Sexual Abuse*, *26*(6), 586–609.

Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E.,... & Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International journal of environmental research and public health*, *19*(16), 9960.

Broadhurst, R., & Ball, M. (2021). How the World'S Biggest Dark Web Platform Spreads Millions of Items of Child Sex Abuse Material—and Why It's Hard to Stop. *The Conversation, September*, *2*.

Burgess, A. W., Hartman, C. R., McCausland, M. P., & Powers, P. (1984). Response patterns in children and adolescents exploited through sex rings and pornography. *The American Journal of Psychiatry*, *141*(5), 656–662.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology*, *14*(2), 20–31.

Caffo, E. (2021). *Online Child Sexual Exploitation*. Springer International Publishing.

Calcara, G. (2013). The Role of INTERPOL and Europol in the Fight Against Cybercrime, with Reference to the Sexual Exploitation of Children Online and Child Pornography. *Masaryk University journal of law and technology*, 7, 19–33.

Chasan-Taber, L., & Tabachnick, J. (1999). Evaluation of a child sexual abuse prevention program. *Sexual abuse: A journal of research and treatment*, *11*, 279–292.

Connolly, K. (2021). German police shut one of world's biggest darknet child abuse images sites. https://www.theguardian.com/world/2021/may/03/german-police-shut-one-of-worlds-biggest-darknet-child-abuse-images-sites. Accessed 7 June 2023.

Datareportal (2022). Digital around the world. https://datareportal.com/global-digitaloverview#:~:text=A%20total%20of%205.07%20billion,12%20months%20to%20October%202022. Accessed 12 Dec 2022

De Vries, I., & Goggin, K. E. (2020). The impact of childhood abuse on the commercial sexual exploitation of youth: A systematic review and meta-analysis. *Trauma, Violence, & Abuse*, *21*(5), 886–903.

De Vries, S. (2021). An analysis of law enforcement cooperation in child sex tourism cases involving Thailand and Canada. *Police practice and research*, *22*(2), 1117–1129.

Dearden, T. E., & Tucker, S. E. (2023). Follow the money: Analyzing darknet activity using cryptocurrency and the Bitcoin blockchain. *Journal of Contemporary Criminal Justice*, *39*(2), 257–275.

Deeb-Swihart, J., Endert, A., & Bruckman, A. (2022). Ethical tensions in applications of AI for addressing human trafficking: A human rights perspective. *Proceedings of the ACM on human-computer interaction*, *6*(CSCW2), 1–29.

Dos Santos Lemos Fernandes, S. (2015). *Protecting Children from Cybercrime: Legislative Responses in Latin America to Fight Child Pornography, Online Grooming, and Cyberbullying through Information and Communication Technologies*. World Bank.

Dushi, D. (2018). Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo. *International Review of Law, Computers & Technology*, *32*(1), 80–98.

Dyson, S. F. (2019). Blockchain Investigations-Beyond the 'Money'. *The Journal of The British Blockchain Association*.

El-Kady, R. (2024). The Complex Landscape of Human Trafficking: A Comprehensive Exploration with Emphasis on Legal Safeguards for Victims in Egyptian and Arab Legislation. In G. Borges, A. Guerreiro, & M. Pina (Eds.), *Modern Insights and Strategies in Victimology* (pp. 118–140). IGI Global. https://doi.org/10.4018/979-8-3693-2201-7.ch006

El-Kady, R. (2025). Early Marriage as a Model of Child Trafficking: Exploring the Legal Safeguards to Victims. In *Social, political, and health implications of early marriage* (pp. 291–326). IGI Global Scientific Publishing.

El-Kady, R., Ertuğrul, D. C., Elçi, A. (2024). Leveraging artificial intelligence to combat illicit activities on the dark web: A descriptive analytical study. In *Multifaceted uses of cutting-edge technologies and social concerns* (pp. 365–392). IGI Global.

El-Kady, R., Hassanien, A. E., Rizk, R. Y., Darwish, A., Alshurideh, M. T. R., Snášel, V., Tolba, M. F. (2025). Proceedings of the 11th international conference on advanced intelligent systems and informatics (AISI 2025). In *Leveraging artificial intelligence for enhanced detection and mitigation of illicit activities on the dark web* (pp. 79–89). Springer Nature.

El-Kady, R. Uddin, E. (2024). Early marriage as a model of child trafficking: Exploring the legal safeguards to victims. In *Social political and health implications of early marriage early marriage* (pp. 291–326). IGI Global.

Escortell, R., Delgado, B., & Martínez-Monteagudo, M. C. (2020). Cybervictimization, self-concept, aggressiveness, and school anxiety in school children: A structural equations analysis. *International Journal of Environmental Research and Public Health*, *17*(19), 7000.

Eurostat (2022) Digital economy and society statistics—households and individuals. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economyand_society_statistics_-_households_and_individuals. Accessed 12 Dec 2022

Finkelhor, D. (2009). The prevention of childhood sexual abuse. *The future of children*, 169–194.

Fisher, B. W., Gardella, J. H., & Teurbe-Tolon, A. R. (2016). Peer cybervictimization among adolescents and the associated internalizing and externalizing problems: A meta-analysis. *Journal of youth and adolescence*, *45*, 1727–1743.

Fonhof, A. M., van der Bruggen, M., & Takes, F. W. (2019). Characterizing critical players in child exploitation networks on the dark net. In *Complex Networks and Their Applications VII: Volume 2 Proceedings The 7th International Conference on Complex Networks and Their Applications COMPLEX NETWORKS 2018 7* (pp. 412–423). Springer International Publishing.

Franchino-Olsen, H. (2021a). Frameworks and theories relevant for organizing commercial sexual exploitation of children/domestic minor sex trafficking risk factors: A systematic review of proposed frameworks to conceptualize vulnerabilities. *Trauma, Violence, & Abuse*, *22*(2), 306–317.

Franchino-Olsen, H. (2021b). Vulnerabilities relevant for commercial sexual exploitation of children/domestic minor sex trafficking: A systematic review of risk factors. *Trauma, Violence, & Abuse*, *22*(1), 99–111.

Fryda, C. M., & Hulme, P. A. (2015). School-based childhood sexual abuse prevention programs: An integrative review. *The Journal of School Nursing*, *31*(3), 167–182.

G. Westlake, B., & Bouchard, M. (2016). Criminal careers in cyberspace: Examining website failure within child exploitation networks. *Justice Quarterly*, *33*(7), 1154–1181.

Gannon, C., Blokland, A. A., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie*, *17*(4), 353–365.

Gannoni, A., Voce, A., Napier, S., Boxall, H., & Thomsen, D. (2023). *Preventing child sexual abuse material offending: An international review of initiatives.* Australian Institute of Criminology.

Geldenhuys, K. (2017). International training highlights the shocking reality of computer-facilitated crimes against children. *Servamus Community-based Safety and Security Magazine*, 110, 20–22.

Guan, S. S. A., & Subrahmanyam, K. (2009). Youth Internet use: risks and opportunities. *Current Opinion in Psychiatry*, *22*(4), 351–356.

Henry, C. (2020). Designing effective digital advertisements to prevent online consumption of child sexual exploitation material. *Journal of child sexual abuse*, *29*(8), 877–899.

Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, *30*(6), 687–698.

Holfeld, B., & Leadbeater, B. J. (2018). The interrelated effects of traditional and cybervictimization on the development of internalizing symptoms and aggressive behaviors in elementary school. *Merrill-Palmer Quarterly*, *64*(2), 220–247.

Holt, T. J., Cale, J., Leclerc, B., & Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression and violent behavior*, *55*, 101464.

Holt, T. J., Lee, J. R., & Griffith, E. (2023). An assessment of cryptomixing services in online illicit markets. *Journal of Contemporary Criminal Justice*, *39*(2), 222–238.

Insoll, T., Ovaska, A., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *The Journal of Online Trust and Safety*, *1*(2).

Islam, M., Mahmood, A. N., Watters, P., & Alazab, M. (2019). Forensic detection of child exploitation material using deep learning. *Deep learning applications for cyber security*, 211–219.

Ivasyuk, O. (2021). Criminological features of cybercrime against minors. *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia.* https://doi.org/10.35750/2071-8284-2021-4-73-77.

Jadimath, P. (2023). ROLE OF CYBER SECURITY IN WOMEN AND CHILD PROTECTION. *International Journal of Engineering Applied Sciences and Technology*. https://doi.org/10.33564/ijeast.2023.v07i10.022.

Jang, Y., & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. *Children*, *10*(8), 1415.

Kahimise, J., & Shava, F. B. (2019, November). An analysis of children's online activities and behaviours that expose them to cybercrimes. In *2019 27th Telecommunications Forum (TELFOR)* (pp. 1–4). IEEE.

Kalaida, I. (2021). The possibilities of blockchain technologies in the investigation of criminal offenses committed into the cyber space. *INFORMATION AND LAW*

Kenny, M. C., Capri, V., Ryan, E. E., & Runyon, M. K. (2008). Child sexual abuse: from prevention to self-protection. *Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect*, *17*(1), 36–54.

Kierkegaard, S. (2008). Cybering, online grooming and ageplay. *Computer Law & Security Review*, *24*(1), 41–55.

Kiss, L., Yun, K., Pocock, N., & Zimmerman, C. (2015). Exploitation, violence, and suicide risk among child and adolescent survivors of human trafficking in the Greater Mekong Subregion. *JAMA pediatrics*, *169*(9), e152278–e152278.

Kloess, J. A., & van der Bruggen, M. (2023). Trust and relationship development among users in Dark Web child sexual exploitation and abuse networks: a literature review from a psychological and criminological perspective. *Trauma, violence, & abuse*, *24*(3), 1220–1237.

Kumar, S. (2021). The Deep Web and Children Cyber Exploitation: Criminal Activities and Methods–Challenges of Investigation: Solutions. In *Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities* (pp. 19–41). IGI Global.

Kumari, M. (2021). Cyber crime and children in digital era. *International Journal of Scientific Research in Science and Technology*, *8*(1), 151–160.

Leiner, M., Peinado, J., Villanos, M. T. M., Lopez, I., Uribe, R., & Pathak, I. (2016). Mental and emotional health of children exposed to news media of threats and acts of terrorism: The cumulative and pervasive effects. *Frontiers in pediatrics*, *4*, 26.

Li, D., Xu, X., Liu, J., Dai, Y., & Chen, X. (2021a). Cybervictimization and adjustment in late childhood: Moderating effects of social sensitivity. *Journal of Applied Developmental Psychology*, *73*, 101258.

Li, M., Chen, Y., Lal, C., Conti, M., Alazab, M., & Hu, D. (2021b). Eunomia: Anonymous and secure vehicular digital forensics based on blockchain. *IEEE Transactions on Dependable and Secure Computing*, *20*(1), 225–241.

Li, S., Qin, T., & Min, G. (2019). Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, *6*(6), 1433–1441.

Lissak, G. (2018). Adverse physiological and psychological effects of screen time on children and adolescents: Literature review and case study. *Environmental research*, *164*, 149–157.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635–654.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online?. *European Journal of Communication*, *29*(3), 271–288.

Marcum, C. D., & Higgins, G. E. (2011). Combating child exploitation online: Predictors of successful ICAC task forces. *Policing: a journal of policy and practice*, *5*(4), 310–316.

Martin, M. (2021). Computer and Internet use in the United States: 2018. *American Community Survey Reports.*

McDool, E., Powell, P., Roberts, J., & Taylor, K. (2020). The internet and children's psychological wellbeing. *Journal of health economics*, *69*, 102274.

McNicol, S. (2016). Responding to concerns about online radicalization in UK schools through a radicalization critical digital literacy approach. *Computers in the Schools*, *33*(4), 227–238.

Mirza, M. M., Ozer, A., & Karabiyik, U. (2022). Mobile cyber forensic investigations of Web3 wallets on Android and iOS. *Applied Sciences*, *12*(21), 11180.

Molero, M. M., Martos, Á., Barragán, A. B., Pérez-Fuentes, M. C., & Gazquez, J. J. (2022). Anxiety and depression from cybervictimization in adolescents: A metaanalysis and meta-regression study.

Moses, J. (2023). Evaluating Government Strategies for Child Online Protection. *Advances in Multidisciplinary and scientific Research Journal Publication.*

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. *Ieee Access*, *8*, 171796–171819.

Nowicka, J., & Zaroślak, M. (2021). Activities for protection of young cyberspace users. *Rocznik Bezpieczeństwa Morskiego*, *15*, 1–16.

Nukusheva, A., Zhamiyeva, R., Shestak, V., & Rustembekova, D. (2022). RETRACTED ARTICLE: Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. *Security Journal*, *35*(3), 893–912.

Núñez-Gómez, P., Larrañaga, K. P., Rangel, C., & Ortega-Mohedano, F. (2021). Critical analysis of the risks in the use of the internet and social networks in childhood and adolescence. *Frontiers in psychology*, *12*, 683384.

oglu Macidov, S. T. (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. *Futurity Economics&Law*, *3*(3), 80–95.

Owen, G. & Savage, O. (2015). The Tor Darknet. Global Commission on Internet Governance, London.

Paquette, S., Chopin, J., & Fortin, F. (2022). Child sexual exploitation material offenders, one-size-fits-all for? Exploring tailored clinical dimensions based on cognitive and behavioural criminogenic factors. *Criminal Behaviour and Mental Health*, *32*(2), 100–113.

Pendergast, K. (2023). Protecting Children Online: Strategies for a Safer Future. *Ubiquity Proceedings*, *3*(1).

Pereda, N. (2013). Systematic review of the psychological consequences of terrorism among child victims. *International review of victimology*, *19*(2), 181–199.

Powell, M., Cassematis, P., Benson, M., Smallbone, S., & Wortley, R. (2014). Police officers' strategies for coping with the stress of investigating Internet child exploitation. *Traumatology: An International Journal*, *20*(1), 32.

Prichard, J., Wortley, R., Watters, P. A., Spiranovic, C., Hunn, C., & Krone, T. (2022). Effects of automated messages on internet users attempting to access "barely legal" pornography. *Sexual Abuse*, *34*(1), 106–124.

Quayle, E. (2020, December). Prevention, disruption and deterrence of online child sexual exploitation and abuse. In *Era Forum* (Vol. 21, No. 3, pp. 429–447). Berlin/Heidelberg: Springer Berlin Heidelberg.

Rafferty, Y. (2008). The impact of trafficking on children: Psychological and social policy perspectives. *Child Development Perspectives*, *2*(1), 13–18.

Rajamäki, J., Lahti, I., & Parviainen, J. (2022). OSINT on the Dark Web: Child Abuse Material Investigations.

Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child abuse & neglect*, *96*, 104080.

Rimer, J. R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. *Child Abuse & Neglect*, *90*, 160–173.

Romaniuk, S. G. (2000). Using intelligent agents to identify missing and exploited children. *IEEE Intelligent Systems and Their Applications*, *15*(2), 27–30.

Rose, C. A., & Tynes, B. M. (2015). Longitudinal associations between cybervictimization and mental health among US adolescents. *Journal of Adolescent Health*, *57*(3), 305–312.

Russell, D., Higgins, D., & Posso, A. (2020). Preventing child sexual abuse: A systematic review of interventions and their efficacy in developing countries. *Child abuse & neglect*, *102*, 104395.

Russo, D., & Parodi, M. (2021). The Protection of Children against Cybercrimes and Cyberbullying: International and European Obligations to Criminalize and the Uncertain Prospects of their Implementation in the Italian Legal System. *International Criminal Law Review*, *21*(4), 767–783.

Ryckman, L. F., Guerra, C., & Finch, A. (2020). Strategies to prevent online sexual abuse of children. *Social Science Protocols*, *3*, 1–7.

Savirimuthu, J. (2011). The EU, online child safety and media literacy. *The International Journal of Children's Rights*, *19*(3), 547–569.

Seigfried-Spellar, K. C. (2018). Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations. *Journal of Police and Criminal Psychology*, *33*, 215–226.

Shetty, S., Shinde, K., Shelke, D., Garje, R., & Mahtre, P. (2023). Crime Evidence Over Blockchain. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*

Sidera, F., Serrat, E., & Rostan, C. (2021). Effects of cybervictimization on the mental health of primary school students. *Frontiers in public health*, *9*, 588209.

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm?. *Computers in human behavior*, *29*(1), 40–50.

Stewart, J., & Witte, T. H. (2020). Secondary trauma and parenting practices in internet crimes against children task force investigators. *American journal of criminal justice*, *45*(6), 1080–1099.

Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, *491*, 151–165.

Tzokov, P. (2019). PERSONALITIES AND PSYCHOLOGICAL FEATURES OF PERPETRATORS OF COMPUTER CRIMES AGAINST CHILDREN. *KNOWLEDGE-International Journal*, *31*(6), 1845–1850.

Van Der Bruggen, M., & Blokland, A. (2021). A crime script analysis of child sexual exploitation material fora on the darkweb. *Sexual Abuse*, *33*(8), 950–974.

Van Der Bruggen, M., & Blokland, A. (2022). Profiling darkweb child sexual exploitation material forum members using longitudinal posting history data. *Social Science Computer Review*, *40*(4), 865–891.

Vásquez-Correa, J. C., & Álvarez Muniain, A. (2023). Novel speech recognition systems applied to forensics within child exploitation: Wav2vec2. 0 vs. whisper. *Sensors*, *23*(4), 1843.

Vieno, A., Gini, G., Lenzi, M., Pozzoli, T., Canale, N., & Santinello, M. (2015). Cybervictimization and somatic and psychological symptoms among Italian middle school students. *The European Journal of Public Health*, *25*(3), 433–437.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, *50*, 303–313.

Voicu, S. N., & Crăciun, I. (2023). Preventive online safety education for teenagers. *International Journal of Legal and Social Order*, *3*(1).

Vrubliauskaitė, K. (2018). Psychological factors increasing the risk for adolescent girls to become victims of human trafficking: A systematic review. *Socialinis darbas*, *16*(1), 129–138.

Walsh, K., Zwi, K., Woolfenden, S., & Shlonsky, A. (2018). School-based education programs for the prevention of child sexual abuse: A Cochrane systematic review and meta-analysis. *Research on social work practice*, *28*(1), 33–55.

Wang, Y., Arief, B., Franqueira, V. N. L., Coates, A. G., & Ó Ciardha, C. (2023, June). Investigating the Availability of Child Sexual Abuse Materials in Dark Web Markets: Evidence Gathered and Lessons Learned. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference* (pp. 59–64).

Westlake, B. G., & Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social science research*, *59*, 23–36.

Wise J (2022). How many people use the dark web in 2022? Secret Stats. https://earthweb.com/how-many-people-use-the-dark-web/. Accessed 12 Dec 2022

Wood, L. C. (2020). Child modern slavery, trafficking and health: a practical review of factors contributing to children's vulnerability and the potential impacts of severe exploitation on health. *BMJ paediatrics open*, *4*(1).

Woodhams, J., Kloess, J. A., Jose, B., & Hamilton-Giachritsis, C. E. (2021). Characteristics and behaviors of anonymous users of dark web platforms suspected of child sexual offenses. *Frontiers in Psychology*, *12*, 623668.

Yang, C. C., Ma, E. T., & Kao, D. Y. (2021, February). Sexual offenses against children: Social learning theory and Dark Web reinforcement. In *2021 23rd International Conference on Advanced Communication Technology (ICACT)* (pp. 449–454). IEEE.

Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016, September). Surfacing collaborated networks in dark web to find illicit and criminal content. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 109–114). IEEE.

Zwi, K., Woolfenden, S., Wheeler, D., O'Brien, T., Tait, P., & Williams, K. (2007). School-based education programmes for the prevention of child sexual abuse. *Campbell Systematic Reviews*, *3*(1), 1–40.

"Artificial Intelligence and Digital Sexual Exploitation of Children on the Dark Web: A Study of Challenges and Mechanisms"



Sameh El-Saeed

1 Introduction

- The rapid evolution of artificial intelligence has created a dual-use dilemma in cyberspace: while AI technologies offer promising tools for detecting and combating online child sexual exploitation, they are simultaneously exploited by offenders to generate, conceal, and distribute abusive content on the dark web. This chapter explores the intersection between AI and the digital sexual exploitation of children, focusing on the challenges posed by deepfake technologies, anonymization techniques, and automated distribution systems. It also examines the mechanisms—technical, legal, and institutional—through which AI can be leveraged to strengthen investigations, enhance victim identification, and disrupt criminal networks operating in hidden layers of the internet (Europol 2023).
- The phenomenon of Digital Sexual Exploitation of Children (DSEC) has intensified with the expansion of online anonymity tools and encrypted networks, particularly within the Dark Web. This hidden layer of the internet has become a breeding ground for illicit marketplaces and forums dedicated to child sexual abuse material, enabling offenders to exchange, produce, and distribute content with relative impunity. The convergence of DSEC and Dark Web platforms poses complex challenges for law enforcement, as traditional investigative methods often fall short in penetrating encrypted communications and anonymized digital environments (Latonero 2019).
- Human Trafficking Overview: Human trafficking is defined as one of the major global crimes that threaten human rights. This crime takes multiple forms, such as forced labor, sexual exploitation, and illegal organ trade. Despite international

S. El-Saeed (✉)
Assistant Professor at Police Science Department-Criminal Justice College-Naif Arab University for Security Sciences, University in Riyad, Riyad, Saudi Arabia
e-mail: dr_samehelsayed@hotmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_11

and local efforts to combat this issue, criminal networks continue to exploit technological advancements to enhance their activities and secure illegal profits.

- **Dark Web**: The dark web is a platform used by human traffickers due to its anonymity and the fact that users can communicate without leaving digital traces. It has become a haven for illegal activities such as human trafficking (https://www.socialbakers.com, 2021).
- **Artificial Intelligence (AI)**: AI is increasingly playing a crucial role in combating cybercrimes, including human trafficking. AI technologies, such as big data analysis, machine learning, and pattern recognition, help track illegal activities and uncover the identities of criminals hiding in the dark corners of the internet.
- The proliferation of online child sexual abuse and exploitation poses a significant global threat to children. In 2023, the US National Center for Missing and Exploited Children (NCMEC) reported over 36.2 million instances of suspected child sexual exploitation, reflecting a 72% increase from the 21 million reports received in 2020. One of the most alarming forms of this exploitation is the creation, distribution, and consumption of child sexual abuse material (CSAM), which includes images, videos, live-streams, or other media depicting real or simulated abuse. This type of exploitation is especially damaging as victims are continuously re-traumatized whenever the material is viewed or shared, leaving a lasting psychological impact.
- Recent research conducted by Protect Children reveals that CSAM is readily available on the surface web, particularly on pornography websites and social media platforms. Offenders frequently exploit popular social media sites and encrypted messaging apps to search for, view, and distribute this illegal content. Moreover, new technologies such as Artificial Intelligence (AI) and Extended Reality (XR) are being misused by perpetrators not only to produce and share CSAM but also to engage in other forms of online child sexual exploitation, such as grooming and sexual extortion.
- This statement delves into the technological abuse involved in online child sexual abuse and exploitation and provides detailed recommendations in Annex 1. These recommendations are directed toward stakeholders in the tech industry and other relevant actors, aiming to curb the spread of CSAM and effectively combat this growing form of exploitation.

2 Introduction 1

Human trafficking is one of the most dangerous crimes facing societies around the world, posing a significant threat to human dignity and human rights. This crime includes various forms, such as forced labor, sexual exploitation, and illegal organ trade. Despite international and local efforts to combat this issue, criminal networks exploit technological developments to strengthen their operations and secure illegal profits (https://www.unodc.org 2023).

Among the tools facilitating these illicit activities, the **dark web** is at the forefront of the platforms relied upon by human traffickers. This network, which operates anonymously and allows users to communicate without leaving any digital traces, has become fertile ground for numerous illegal activities, including human trafficking. Criminal gangs exploit the dark web's features to promote and sell victims far from the scrutiny of legal and regulatory authorities.

With the rise of this cyber threat, **Artificial Intelligence (AI)** has emerged as a powerful tool in combating cybercrimes, including human trafficking through the dark web. AI relies on technologies like big data analysis, machine learning, and pattern recognition, enabling authorities to track illegal activities and uncover the identities of those involved, even as they continuously attempt to hide in the darkest corners of the internet.

This research will detail how the dark web is used to facilitate human trafficking and explore the growing role AI plays in detecting and effectively combating these activities.

3 Introduction 2

- Human trafficking is considered one of the most dangerous crimes confronting the international community today. It is classified as a transnational crime that targets the most vulnerable groups in society. According to reports from the United Nations and non-governmental organizations, millions of people are forced each year into labor exploitation, sexual exploitation, or illegal organ donation, causing immense suffering and violating basic human rights and dignity (Zelenskyy 2021).

This phenomenon is complex and diverse, as criminal gangs exploit economic and social vulnerabilities in certain countries and use advanced technologies to escape legal accountability. Despite efforts made by governments and international organizations to combat this crime, the scale of the problem remains vast, requiring more effective solutions.

- In this context, the **dark web** has emerged as a key tool used by criminal gangs to facilitate human trafficking operations and conceal their tracks. The dark web is a hidden part of the internet, accessible only through certain software that allows users to browse anonymously. Due to these features, the dark web has become a safe haven for various illegal activities, including drug trafficking, arms sales, distribution of pornography, and human trafficking. In fact, the dark web allows traffickers to communicate with each other and with their clients away from legal oversight, where people are sold and bought as commodities, making it extremely difficult for authorities to track and stop these crimes (https://www.satimagingcorp.com 2024).

- With significant technological advancements in recent years, **AI** has become a promising tool in confronting this type of complex cybercrime. AI, a set of technologies that simulate human mental capabilities such as learning, reasoning, and adaptation, is now able to process vast amounts of data and analyze it with exceptional speed. AI technologies such as machine learning and big data analysis can play a pivotal role in detecting suspicious patterns on the internet, including illegal activities on the dark web. By utilizing these technologies, it is possible to trace financial transactions, decrypt anonymous communications, and even identify individuals involved in human trafficking crimes, contributing to bringing them to justice (Pelton and Madry 2020, p. 5).

This research aims to explore the relationship between the use of the dark web in human trafficking operations and the critical role AI can play in combating these activities. We will discuss how the dark web is exploited by criminals and the mechanisms through which AI can reduce this crime and achieve justice for victims.

4 Research Problem

- **Challenges Posed by Human Trafficking Through the Dark Web**: Encryption, difficulty in tracking identities, and high levels of secrecy.
- **The Need for Advanced Technologies Like AI**: To curb these activities on the dark web and achieve effective results in tracking and combating this phenomenon.

Research Questions

When studying human trafficking through the dark web and combating it using AI technologies, several complex issues arise that hinder efforts to uncover these illegal activities. These problems span technical, legal, and ethical aspects, imposing significant challenges on both international and local investigations. The following are the most prominent issues:

1. **Encryption and Decryption Challenges**: One of the biggest challenges in combating human trafficking through the dark web is the heavy reliance on advanced encryption. The encryption techniques used in the dark web make decryption of communications between criminals nearly impossible with traditional methods.
2. **Anonymous Identity and Tracking Difficulty**: A key feature of the dark web is the anonymity it offers its users. Digital identity information is hidden through advanced protocols like **Tor**, allowing criminals to interact and conduct transactions without revealing personal information.

3. **Secretive and Closed Environment**: The dark web operates with high secrecy and closed access, making it challenging for legal authorities to access the required information or infiltrate criminal networks.
4. **Rapid Evolution of Technologies Used on the Dark Web**: The dark web is a constantly changing environment, with criminals continuously adopting the latest technologies to stay ahead of law enforcement.
5. **Lack of International Cooperation and Unified Efforts**: Despite being a global crime, efforts to fight human trafficking often suffer from a lack of coordination between different countries.
6. **Analyzing Big Data and Distinguishing Between Legitimate and Illegitimate Activities**: The dark web is not exclusively used for illegal activities, making it challenging to differentiate between legal and illegal operations.

- **Legal and Ethical Uncertainties**: The use of AI in combating crimes raises legal and ethical questions about privacy, human rights, and surveillance. (https://www.boldbusiness.com 2024)

5 Research Goals

1. Analyze the role of AI in detecting and analyzing activities related to human trafficking on the dark web.
2. Review the technologies and mechanisms used to employ AI to combat this crime.
3. Discuss the challenges and limitations facing AI applications in this context.
4. Provide recommendations to enhance the effectiveness of AI in combating human trafficking.

6 Final Version of the Research Goals

1. Analyze the role of AI technologies in detecting and tracking activities related to human trafficking on the dark web.
2. Review the tools and algorithms used in employing AI to combat human trafficking on the dark web.
3. Discuss the technical and ethical challenges faced by AI applications in combating human trafficking.
4. Provide recommendations to enhance the effectiveness of AI in detecting and combating human trafficking operations on the dark web.

7 Methodology

- **Descriptive and Analytical Methodology**: This method relies on previous studies and the analysis of technological applications in AI used to combat cybercrimes.
- **Quantitative Methodology**: Using data and reports on crimes detected using AI.

8 Proposed Research Methodology

- To carry out research on the role of AI in combating human trafficking on the dark web, it is essential to follow a comprehensive methodology that combines qualitative and quantitative analysis. This methodology should explore the role AI plays, assess the effectiveness of the technologies used, and understand the challenges faced by AI applications in this field. The proposed methodology includes (Beukema 2024):

First: Stages of Sexual Exploitation of Children via the Internet

The internet has enhanced offenders' capabilities to commit crimes related to the sexual exploitation of children, facilitating access to and distribution of child pornography. The internet allows reaching pornographic images from any country in the world, making child pornography accessible anytime and anywhere. It enables direct communication and the sharing of images between users without revealing their identity, particularly providing child pornography at low cost and high quality, with comfortable storage capacities for these materials in various formats such as images, videos, and audio. Additionally, the internet offers interactive real-time experiments to access modified digital images to create synthetic or virtual images.

- The criminalized actions in child exploitation crimes involving online child pornography can be divided into three stages: **Production of Images, Distribution, and Downloading**. Often, the same individuals are involved in all stages, and the primary motive for producers and distributors of child pornography is financial gain rather than sexual pleasure (https://www.boldbusiness.com 2024).

9 Production of Pornographic Material

This involves the creation of pornographic images where offenders gather child pornographic images that have been produced earlier or obtained from old magazines and films. They then professionally reproduce these images to create child-specific pornographic content or record explicit content of themselves. The development in information technology media, such as digital cameras, webcams, and advanced mobile phones, facilitates this process by enabling the production of high-quality images and videos of children.

10 Distribution of Child Pornography

This stage includes uploading and distributing child pornographic content on the internet, stored on website servers, other dedicated servers, or shared servers. Distribution usually occurs through social media groups requesting child pornography. Such crimes may be committed by organized crime groups for profit or by hobbyists who are not interested in financial gain. Child pornographic images are uploaded to the internet via different websites, or they are shared through direct messaging and chat rooms.

11 Downloading Child Pornographic Images

- This phase involves offenders obtaining child pornography via the internet without necessarily storing it on hard drives. Sometimes, individuals receive emails advertising child pornography, or they encounter pop-up links on unrelated websites, which direct them to pornographic content (https://www.statista.com, 2024a, 2024b)

1. **Descriptive Methodology:**

The **descriptive methodology** will be used to describe the phenomenon and the environment in which human trafficking operates on the dark web. The focus will be on:

- **Describing the Dark Web**: Analyzing how the dark web is used as a platform to carry out human trafficking operations, including the main activities and forms of trafficking.
- **Explaining AI Technologies**: Providing a clear explanation of the technologies used to combat cybercrimes, such as big data analysis, machine learning, and pattern recognition.

2. **Analytical Methodology:**

The **analytical methodology** will be used to analyze the information and data collected about the use of AI in combating human trafficking. The analysis will include:

- **Analyzing the Technologies Used**: Studying the various tools and algorithms, such as **Machine Learning** and **Deep Learning**, and how they are used to detect criminal activities.
- **Analyzing the Challenges and Limitations**: Discussing the technical, legal, and ethical challenges hindering the use of AI in this field, such as encryption issues, data protection, and anonymous identities. (https://www.socialbakers.com 2021).

3. **Comparative Methodology:**

The **comparative methodology** involves comparing different AI techniques and evaluating their effectiveness. This includes:

- **Comparing Technologies**: Comparing the various AI tools used to detect human trafficking and determining which ones are more effective on the dark web.
- **Comparing Countries**: Reviewing the efforts of different countries in employing AI to combat human trafficking through the internet and analyzing the effectiveness of these efforts.

4. **Quantitative Methodology:**

In this research, the **quantitative methodology** will also be used to study the data related to the volume of human trafficking operations on the dark web and the impact of AI technologies on reducing these operations. This methodology may include:

- **Big Data Analysis**: Using available data on criminal activities on the dark web to evaluate the practical impact of AI technologies in detecting these activities.
  - **Statistics and Performance Evaluation**: Collecting quantitative data on the success of AI in tracking and detecting these crimes, such as the number of crimes detected or the individuals arrested (Report of UN 2020).

4. **Applied Methodology:**

At this stage, the **applied methodology** will be used to test the practical effectiveness of AI by studying real-life cases or specific models of how AI is used to detect human trafficking crimes. This includes:

- **Case Studies**: Analyzing real cases where AI was used to detect human trafficking operations on the dark web. This study will contribute to a deeper understanding of the effectiveness of the tools and technologies used.
- **Field Applications**: It is also possible to analyze actual applications of AI technologies implemented by law enforcement agencies or international organizations (https://syntheticdrugs.unodc.org 2023).

6. **Data Collection and Sources:**

- **Literature Review**: Reviewing previous studies and academic articles that have addressed issues related to the dark web, human trafficking, and AI technologies.
- **Secondary Sources**: Relying on reports from human rights organizations, law enforcement data, and government agencies regarding human trafficking and AI usage.

– **Primary Sources**: Conducting interviews or surveys with experts in cybersecurity, AI, and law enforcement to gain in-depth perspectives on practical applications and challenges (Swihart et al. 2022, p. 295).

- **Child Sexual Abuse and Exploitation in the Digital Age and Respective Challenges**

The Surface Web, Social Media Platforms, and End-To-End Encryption

- Recent studies have shown that child sexual abuse material (CSAM) is accessible on the surface web, including social media platforms. A survey conducted by Protect Children, which involved individuals searching for CSAM on dark web search engines, revealed that 77% of respondents encountered CSAM or links to such material on the surface web. These included pornography websites (32%), social media platforms (29%), and messaging applications (12%). The most frequently cited platforms where CSAM was found were Instagram, X (formerly Twitter), Discord, and TikTok.
- Recommendation algorithms, like those on TikTok and Instagram, have been found to promote "self-generated" CSAM and facilitate its trading. This material is often created unintentionally by minors and is non-consensual, typically arising from grooming or manipulation by offenders. Offenders exploit social media algorithms by falsifying their age to resemble a child or adolescent, thus prompting the system to suggest content created by minors with similarly falsified ages. This age falsification allows offenders to easily gain a child's trust by pretending to be a peer, which can lead to grooming and sexual extortion, and ultimately, further abuse.
- Additionally, encrypted messaging apps like Telegram and WhatsApp are popular among CSAM offenders for distributing and viewing such material. These apps use end-to-end encryption (E2EE), which ensures that only the communicating parties can access the content of their messages. Features like secret chats, self-destruct messages, the ability to edit or delete messages for all users, and private groups create an environment that facilitates the exchange of CSAM with a "minimal digital footprint." The encrypted nature of these platforms makes CSAM nearly impossible to detect, which complicates the removal and regulation of this harmful material and allows it to
- proliferate unchecked.

12 Online Gaming

Online gaming platforms that feature player-to-player interaction are increasingly exploited by offenders to establish contact and "befriend" children. One of the primary dangers associated with online games is sexual extortion. While we seek a more appropriate term, we continue to use "self-generated" CSAM, acknowledging its limitations and providing additional remarks.

Children often overlook the real dangers present in virtual worlds, as they do not expect threats in these environments, leading them to feel safer on these platforms. This normalization of communication with strangers online can be exploited by perpetrators. Since revealing personal information is typically not required, offenders can easily conceal their true identities and deceive minors. This can lead to grooming—a form of violence that develops slowly and is difficult to detect—which may then escalate into other forms of child sexual abuse and exploitation.

13 Anonymity on the Dark Web

Similar to end-to-end encryption (E2EE), the dark web offers users anonymity and the ability to evade surveillance, creating a haven for illegal activities, including the proliferation of CSAM. Reports indicate that 21 out of 26 Tor search engines provide results related to CSAM, with four of these engines actively promoting and advocating for such material. Approximately 20% of unique websites hosted on the Tor network share CSAM.

Furthermore, a significant portion of search sessions within these domains—about 11%—specifically seeks CSAM. This sheer volume and demand for CSAM on the dark web have effectively overwhelmed law enforcement agencies, making it challenging to identify and remove all child sexual abuse content without the aid of technology. Additionally, forums on the dark web serve as hubs for like-minded individuals to connect, validate each other's actions, and share CSAM, further perpetuating the sexual abuse and exploitation of children.

Tracking down offenders while adhering to legal and ethical standards has become a significant challenge for law enforcement. They must maintain a delicate balance between protecting individuals' rights to privacy and combating illegal activities.

7. **Legal and Ethical Analysis:**

This stage of the research will review the **legal** and **ethical dimensions** related to using AI to combat crimes, determining the laws and regulations governing the application of these technologies. This includes:

- **Analyzing International and Local Laws**: Studying the legislation related to privacy protection and data governance in the context of AI usage.
- **Ethical Standards:** Analyzing the ethical challenges involved in using surveillance and AI technologies to detect crimes while respecting human rights. (https://www.satimagingcorp.com 2024).

14 The Final Recommendations

Based on the results derived from the descriptive and analytical analyses, practical recommendations will be made to improve and develop the use of AI in combating human trafficking. These recommendations will be based on the data collected and analyzed to provide effective strategies for addressing the challenges.

15 Work Plan

1. **Literature Review**: Begin by reviewing previous studies related to human trafficking, the dark web, and AI usage in combating cybercrime.
2. **General Description and Analysis**: Use the descriptive methodology to describe the dark web and AI technologies used in this context.
3. **Comparative Analysis**: Compare different tools and algorithms used to combat these crimes (https://www.satcen.europa.eu, 2024)'.
4. **Legal and Ethical Challenges**: Analyze the challenges faced in applying AI, whether technical, legal, or ethical.
5. **Case Studies and Field Applications**: Examine real-world examples of AI being used to detect these crimes.
6. **Final Recommendations**: Provide recommendations based on the analysis to enhance the effectiveness of AI in combating human trafficking through the dark web.

16 Main Research Areas

1. **Overview of the Dark Web and Its Role in Cybercrime**:
– Defining the dark web and how it can be accessed.
– The use of the dark web in human trafficking crimes.
– The difficulty of detecting crimes on this network.

Section 1: Overview of the Dark Web and Its Role in Cybercrime

1.1 **Definition of the Dark Web and How to Access It:**

- The **dark web** is the hidden part of the internet that cannot be accessed through traditional browsers or search engines such as Google or Bing. It is a small portion of the deep web, which includes all websites requiring authentication or that cannot be indexed by search engines. Unlike the surface web used by most people, the dark web is concealed behind complex encryption protocols, making it nearly impossible to access or track users without specialized tools (https://syntheticdrugs.unodc.org, 2023).
- Accessing the dark web requires tools like the **Tor** browser, which is used to hide users' identities by encrypting their data and routing it through multiple nodes (servers) worldwide, making it difficult for any external party to track the original source of communication. All data traffic is encrypted several times and routed through a chain of volunteers, making it almost impossible to trace the true identity of the user. Additionally, the dark web uses protocols like **Onion Routing**, which enhances user anonymity and encryption (https://www.fastcompany.com 2024).

17 Difference Between the Dark Web and the Deep Web

- **Deep Web**: Includes content not indexed on the internet, such as library databases, online banking systems, or academic platforms. These contents are not illegal.
- **Dark Web**: A subset of the deep web, mainly associated with illegal activities due to the anonymity and privacy it offers.

1.2 The Use of the Dark Web in Human Trafficking Crimes:

- Human trafficking is one of the most dangerous crimes carried out on the dark web. Hidden platforms on this network are used to promote and sell victims of human trafficking, whether for sexual exploitation, forced labor, or even the illegal trade of human organs. The dark web provides a safe environment for traffickers to avoid law enforcement surveillance, where they rely on anonymous advertisements and encrypted forums to negotiate sales or organize deals between buyers and sellers (https://www.satcen.europa.eu 2024)'.

There are several ways in which the dark web is exploited for human trafficking:

1. **Secret Advertisements**: Criminals post hidden advertisements related to human trafficking victims using encrypted language or specific forums on the dark web. These advertisements are often coded or disguised to avoid detection.

- **Encrypted Forums**: Traffickers communicate with each other through encrypted forums that are difficult for law enforcement agencies to monitor or infiltrate. (EU Policy Cycle 2022).
- **Cryptocurrency Payments**: Payments for human trafficking operations are often conducted using cryptocurrencies such as **Bitcoin** or **Monero**, making it difficult for financial institutions or surveillance agencies to track the money flow (Report of UN 2020).

Despite attempts by authorities to infiltrate these networks, traffickers continuously evolve their methods to protect their identities and operations. The secrecy provided by the dark web makes it extremely difficult for authorities to monitor these activities, allowing criminals to manage their operations away from scrutiny.

1.3 The Difficulty of Detecting Crimes on the Dark Web:

- Detecting crimes on the dark web, including human trafficking, presents a tremendous challenge for law enforcement agencies worldwide. Several factors contribute to the difficulty in uncovering these crimes: (Kobielus 2020).
- **Advanced Encryption**: All communications and data exchanged on the dark web are encrypted, meaning that even if suspicious activities are detected, decrypting the information can take years using conventional methods. Moreover, the traffic

is encrypted at every stage, which means that even partial leaks of information will not lead to a full disclosure of criminal activities (https://www.boldbusiness.com 2024).

2. **Anonymity**: The anonymity of users is fully protected on the dark web through technologies such as **Tor** and **VPNs**, making it extremely difficult to track users or uncover their identities. Additionally, criminals often rely on cryptocurrencies such as **Monero**, which offer greater privacy compared to Bitcoin, further complicating financial tracking (Swihart et al., 2022).

- **Complex Infrastructure**: Even if authorities manage to access certain websites on the dark web, these sites are usually well-protected with strong passwords and complex login mechanisms, preventing unauthorized access. Moreover, criminals can shut down or relocate their sites within minutes if they suspect a threat (https://www.adfsolutions.com 2024).

3. **Rapid Development of Criminal Techniques**: Criminals on the dark web constantly learn from each other and develop new technologies to stay ahead of law enforcement. This means that any new techniques employed by authorities to combat dark web crimes can be quickly adapted to or neutralized by criminals.

Section 2: AI Applications in Combating Cybercrime

2.1 **Analyzing Encrypted Texts and Conversations on the Dark Web**

- **Pattern and Suspicious Data Recognition Techniques**
- **Deep Neural Networks and Machine Learning Techniques to Detect Human Trafficking Activities**
- **Analyzing Encrypted Texts and Conversations on the Dark Web:** (Michailidis and Vouyioukas 2022)

One of the most important techniques AI uses to combat cybercrime is analyzing encrypted texts and conversations. This type of analysis relies on **Natural Language Processing (NLP)**, a subfield of AI concerned with understanding and analyzing written or spoken texts.

18 How Text Analysis Works

1. **Data Collection**: The process begins by collecting large amounts of text and conversation data from the dark web's forums or secret commercial websites used for human trafficking. This requires accessing data using online intelligence techniques, including **web crawling** tools, which automatically gather text from various sources.

2. **Pattern Recognition**: NLP technologies rely on algorithms capable of extracting linguistic patterns and repetitions from texts. For example, these algorithms can analyze encrypted conversations between traffickers and potential buyers, identifying coded words or symbols used to refer to victims or prices (Jafarbiglu and Pourreza 2022, p. 197).
3. **Context Analysis**: After extracting linguistic patterns, AI analyzes the context in which these words are used. For example, if certain words or phrases are used in conversations related to human trafficking or sexual exploitation, the system alerts investigators to this activity.
4. **Machine Translation**: Since many conversations on the dark web take place in multiple languages, machine translation tools play a critical role in translating encrypted texts into a language understandable to investigators.

2.2 Pattern Recognition and Suspicious Data Detection Techniques:

- Pattern recognition is at the core of AI's efforts to combat cybercrime. These techniques extract recurring or unusual patterns in large datasets. In the context of combating human trafficking, these techniques can help uncover illegal activities on the dark web based on user behavior or communication patterns (https://www.satimagingcorp.com 2024).

19 How Pattern Recognition Works

1. **Big Data Collection**: AI requires vast amounts of data for analysis. Data is collected from multiple sources, such as financial transaction logs using cryptocurrencies, human trafficking forums, and other suspicious activities on the dark web.
2. **User Behavior Analysis**: AI analyzes user behavior on the dark web, such as the frequency of visits, posting frequency, patterns of interaction with other users, and the types of transactions they conduct. These patterns can reveal criminal activity. For example, if a user repeatedly visits certain sites or advertises illegal products, it may indicate suspicious activity.
3. **Detecting Suspicious Financial Activities**: AI can track financial transactions using cryptocurrencies. These techniques help identify unusual or suspicious financial transactions, such as large or frequent transfers to certain addresses, which may indicate activities related to human trafficking.

2.3 Deep Neural Networks and Machine Learning Techniques for Detecting Human Trafficking Activities:

Deep neural networks (DNNs) and machine learning (ML) techniques are essential tools for detecting illegal activities online, including human trafficking. These techniques rely on training algorithms to recognize complex patterns and analyze interconnected data.

20 How Deep Neural Networks Work

1. **Training with Data**: The process begins with training neural networks on vast amounts of data related to criminal activities, such as images, texts, and financial transactions. The model learns from this data how to identify patterns associated with human trafficking, such as images of victims or messages about trafficking (Monitoring Global Threats 2012).
2. **Continuous Learning**: Over time, neural networks become more accurate in detecting criminal activities as they adapt to the new data introduced continuously. For example, human trafficking patterns may evolve, but AI can learn and adapt to these changes.
3. **Image and Video Recognition**: DNNs are used to recognize visual content related to human trafficking. For instance, if images or videos of victims are posted on the dark web, AI can analyze these images and determine whether they are linked to human trafficking activities.

Section 3: AI Tools and Technologies Used to Combat Human Trafficking

- **Language Translation and Analysis Technologies to Identify Content Related to Human Trafficking**
- **Using Big Data Analysis to Track Suspicious Activities**
- **Detecting Ads or Posts Related to Human Trafficking Online**

3.1 Language Translation and Analysis Technologies to Identify Content Related to Human Trafficking

With human trafficking content being produced in various languages and dialects around the world, the use of **language translation and analysis technologies** has become crucial in uncovering illegal activities. These technologies rely on **Natural Language Processing (NLP)** models and **machine learning** to analyze texts, translate them, and identify linguistic patterns that may indicate suspicious activity (Zhang 2023).

21 How Translation and Language Analysis Works

1. **Machine Translation**: AI platforms rely on algorithms such as **Google Neural Machine Translation (GNMT)** or other neural network-based technologies to translate texts from multiple languages into a language understandable by investigators or law enforcement. Tools like **Microsoft Translator** or **DeepL** are used to convert foreign-language texts into the desired language, with a focus on maintaining context and meaning.

2. **Linguistic Pattern Analysis**: After translation, **NLP** techniques are employed to analyze the texts, searching for suspicious linguistic patterns related to human trafficking activities. For example, phrases related to pricing, locations, or suspicious circumstances are analyzed to understand the context in which they are used.
3. **Recognizing Codes and Masked Expressions**: On the dark web or in criminal online conversations, traffickers may use coded or cryptic language to avoid detection. AI technologies can learn these patterns through **machine learning**, decoding or interpreting these disguised expressions that may be used in human trafficking operations (Pelton and Madry 2020, p. 5).

22 Artificial Intelligence

Artificial Intelligence (AI) has created unique challenges in identifying victims depicted in images, videos, and other representations of sexual violence against children. Recent technological advancements have introduced AI image-generation platforms, where users can input a text prompt, and the AI generates an image based on that input.

Perpetrators misuse AI in various ways, including:

- **Manipulating Photos or Videos**: This includes altering existing Child Sexual Abuse Material (CSAM).
- **Creating New Material**: Generating entirely new, AI-created content that depicts sexual abuse of children.
- **Nudification**: Altering clothed images of children to make them appear naked.
- **De-Aging Algorithms**: Using algorithms that make individuals look younger.

AI-generated CSAM is often promoted within offender communities as a "harm-free" approach, similar to claims that viewing existing CSAM is not harmful as long as they are not actively contacting children or creating new content. This assertion, however, is false. AI-generated CSAM normalizes sexual violence and abuse of children, leading offenders to view it as "just a picture." However, previous research by Protect Children indicates that offenders who frequently consume CSAM are more likely to attempt to contact children, rendering arguments about a "lesser evil" baseless.

Additionally, AI algorithms have advanced to the point where they can generate content that is indistinguishable from real photos and videos, even to trained eyes. This advancement results in wasted law enforcement resources, as authorities increasingly spend time analyzing images to identify children who do not exist. These tools can produce an unlimited number of images offline, leaving offenders with little risk of detection.

Challenges:

- **Linguistic Diversity**: With content in multiple languages and dialects, translation accuracy can be challenging, especially with colloquial or cryptic expressions.
- **Accuracy**: While there have been significant advancements in machine translation technologies, accuracy can still be affected by context or complex sentence structures.

3.2 Using Big Data Analysis to Track Suspicious Activities

With the rapid growth of the volume of data available on the internet, **big data analysis** has become one of the essential tools for detecting suspicious activities, including human trafficking. This process relies on gathering and analyzing vast amounts of data from various sources, including the dark web, surface web, social media platforms, and commercial websites.

23 How Big Data Analysis Works

1. **Data Collection**: The first step involves gathering data from a wide range of sources, including texts, images, videos, and financial information. Data is obtained from dark web sites, social media platforms, and any suspicious activities that may be related to human trafficking.
2. **Behavioral Pattern Analysis**: After collecting the data, **machine learning** and pattern recognition techniques are used to detect behaviors that might indicate human trafficking activities. For example, AI can track user activity, such as frequent visits to suspicious websites or unusual financial transactions using cryptocurrencies.

– **Social Network Analysis**: AI technologies also rely on **social network analysis** to detect links between users who may be involved in human trafficking. AI can identify individuals linked to trafficking victims or potential criminals by studying relationships between online accounts and conversations (Swihart et al. 2022, p. 295)

Challenges:

- **Huge Volume of Data**: Handling vast amounts of data requires significant computational resources and the ability to filter relevant information from noise.
- **Data Diversity**: The data collected can be unstructured, such as texts or unstructured images, making analysis more difficult.

3.3 Detecting Ads or Posts Related to Human Trafficking Online

One of the most critical uses of AI in combating human trafficking is the detection of advertisements or posts that may be related to trafficking, whether on the dark

web or open commercial platforms. AI analyzes ads and posts from illicit online marketplaces or forums used by criminal gangs.

24 How AI Detects Ads

1. **Web Crawling**: In this step, **web crawling** technologies are used to collect ads and posts from various websites on the internet. These tools can scan millions of ads daily across the surface web and dark web.
2. **Image and Text Analysis**: After collecting the ads, **image recognition** and **NLP** techniques are used to analyze the content. AI can identify images that may be related to human trafficking, such as photos of victims or items being advertised as goods.
3. **Content Classification**: After analyzing the text and images, **classification algorithms** are used to determine whether the content contains indicators of human trafficking. Ads are classified into categories, such as those promoting sexual exploitation or forced labor.

Challenges:

- **Complexity in Ads**: Some ads are designed to be indirect or encrypted, making detection more challenging.
- **Adapting to New Techniques**: AI systems must continuously adapt to new methods traffickers use to hide their activities.

Section 4: The Role of International Cooperation and Security Agencies

- **How AI Can Support Collaboration Between Security Agencies Globally**
- **Examples of Existing Projects Using AI to Combat Crimes on the Dark Web (e.g., DARPA Program)**

4.1 How AI Can Support Collaboration Between Security Agencies Globally

The biggest challenge in combating cybercrime, such as human trafficking, is the need for continuous international coordination between different security agencies. Because of the decentralized nature of the dark web and the anonymity it provides, these crimes are often carried out across multiple countries, making it extremely difficult to track criminals. This requires advanced tools that can track illegal activities on a global scale. AI plays a crucial role in facilitating cooperation in several ways.

1. **Analyzing Data Across Borders**: One of the biggest challenges facing law enforcement in combating human trafficking is analyzing the diverse data that comes from multiple sources. The data available on the dark web may include texts, images, videos, and financial data related to cryptocurrency transactions. These datasets vary greatly from one country to another, making manual analysis inefficient.

AI techniques, such as **deep learning** and **machine learning**, can process and analyze these vast datasets quickly. AI models are trained to recognize suspicious patterns in the data that may indicate criminal activities. For example, these models can analyze text conversations on the dark web to extract phrases related to human trafficking or track cryptocurrency flows to identify suspicious transactions (Li et al. 2022, p. 5163).

Through these tools, security agencies can share their findings with other agencies across borders, facilitating coordinated and joint investigations. If a security agency in a particular country detects suspicious activity, this analysis can be shared with law enforcement agencies in other countries in real time, enhancing the speed and efficiency of international investigations.

2. **Smart Profiling and Identifying Suspects**: **Smart profiling** is one of the effective tools AI provides to combat human trafficking. AI can analyze user profiles of suspects and identify suspicious behavioral patterns that may indicate their involvement in human trafficking operations. These patterns include frequent communications with other members of criminal networks or financial activities that indicate unusual transactions.

   AI models can also build digital profiles or "digital fingerprints" for suspected individuals, making it easier to monitor them online. These profiles are continuously updated with each new activity the individual engages in on the web, enhancing security agencies' ability to identify and track individuals across borders.
3. **Joint Coordination and Surveillance**: Effective international coordination requires the presence of **joint surveillance systems** that rely on AI to detect suspicious activities in real-time. These systems can monitor financial transactions or illegal activities in real-time, allowing security agencies to respond quickly to crimes.

4.2 Examples of Existing Projects Using AI to Combat Crimes on the Dark Web

Several global projects use AI to strengthen the capabilities of security agencies in combating cybercrime, especially human trafficking. Below are some notable examples:

1. **DARPA—Memex Program**:

   DARPA, the Defense Advanced Research Projects Agency, developed the **Memex** project, which aims to improve the ability of security agencies to detect crimes on the internet.

The Memex project is a powerful tool that uses AI and machine learning to scan the content of the deep and dark web. The program is primarily used to analyze text and visual content shared on the dark web to identify illegal activities such as human trafficking, drug trade, and weapons sales.

Memex is capable of:

- **Web Crawling**: It searches the deep and dark web for content related to criminal activities that are not indexed by traditional search engines.
- **Pattern Analysis**: It identifies suspicious patterns in texts, images, and videos that may indicate human trafficking or other crimes.
- **Activity Mapping**: It helps security agencies map out criminal activities by analyzing links between websites and users (Gui et al. 2024, p. 327).

2. **THORN Project**:
   The **THORN** project is a non-profit initiative aimed at combating child sexual exploitation and human trafficking using AI. It was developed by a non-governmental organization in collaboration with global law enforcement agencies.

The THORN project relies on AI to analyze suspicious ads and content that may be related to human trafficking. The project uses **machine learning algorithms** to analyze data from the internet and identify content related to the crime.

3. **IBM i2 Analyst's Notebook**:

   IBM i2 Analyst's Notebook is an AI-based analytical system used by law enforcement agencies to analyze complex criminal networks. This program provides advanced analytical tools that can:

– **Map Relationships**: Link different criminal activities and uncover criminal networks involved in human trafficking.
– **Analyze Big Data**: Handle and analyze vast amounts of data from multiple sources to detect suspicious activities.

Section 5: Challenges and Limitations in Using AI to Combat Human Trafficking

- **Technical Challenges, such as Data Encryption and Overcoming Barriers**
- **Ethical Issues Related to Privacy and Individual Rights**
- **The Need for Continuous Updates in AI Technologies to Keep Up with the Dark Web**

5.1 Technical Challenges, Such as Data Encryption and Overcoming Barriers

Data encryption and overcoming barriers are some of the toughest technical challenges faced by law enforcement agencies when using AI to combat cybercrimes on the dark web. The dark web protects users through multiple layers of encryption and secrecy, making it extremely complex for authorities to track or monitor criminal activity.

1. **Data Encryption**:

   The dark web relies on complex encryption protocols such as **Tor**, which hide users' identities and movements across the internet. This encryption makes it difficult for law enforcement or AI systems to access communications between criminals and analyze data in real time.

These networks use **end-to-end encryption**, meaning that messages are encrypted entirely from sender to recipient, and cannot be intercepted or decrypted by third parties, including law enforcement agencies.

2. **Overcoming Barriers**:

   The dark web blocks access to certain content using advanced techniques such as **onion routing**, which makes it difficult for traditional systems and even AI to access certain websites. AI depends on tools like web crawlers to reach content, but some sites are protected by barriers that make access nearly impossible without human intervention or additional advanced tools.

   AI technologies also face additional challenges in gathering data from sources protected by complex firewalls or multi-layer verification systems. Moreover, some criminals use **VPNs** and multiple layers of protection to enhance secrecy, making tracking them even more difficult.

3. **The Rapid Evolution of Encryption Technologies**:

   Criminals on the dark web are constantly developing new methods to protect their activities. For example, some have begun using cryptocurrencies with higher privacy than Bitcoin, such as **Monero** and **Zcash**, making financial tracking more difficult, even using advanced AI technologies.

Possible Solutions:

- **Deep Learning**: **Deep learning** models can be used to analyze financial flows and encrypted conversations, with repeated learning processes to improve their ability to decrypt.
- **Collaboration with Tech Entities**: Law enforcement agencies can collaborate with tech companies to develop new tools capable of decrypting or accessing encrypted data more efficiently.

5.2 Ethical Issues Related to Privacy and Individual Rights

Using AI to combat cybercrimes raises complex ethical questions about the extent of interference in individuals' privacy and rights, whether they are regular internet users or potential criminals.

1. **Invasion of Privacy**:

   With AI's ability to monitor and analyze massive amounts of personal data from the internet, concerns about privacy violations are growing. Technologies such as **facial recognition**, **text analysis**, and **behavioral profiling** may be used to monitor individuals extensively, which could lead to unintended breaches of personal rights.

   Data may be collected from social media platforms, financial transactions, or private conversations as part of investigations into human trafficking, but this could sometimes exceed acceptable legal and ethical limits on privacy.

2. **Misuse of Data**:

There is a risk that data collected for legal or security purposes could be misused, whether by governments or private companies. This could lead to the misuse of personal information collected under the pretext of combating crime.

3. **Bias and Discrimination**:

   AI models rely on historical data to learn patterns and predict future behaviors. If these datasets contain racial or cultural biases, they could lead to unfair predictions or discrimination against certain segments of the population.

   Some models may unfairly target vulnerable groups or communities that have historically faced discrimination, further complicating the ethical issues related to the use of AI in combating crime.

Possible Solutions:

- **Establishing Strict Regulations**: Governments and international organizations must establish strict regulations governing the use of AI in monitoring individuals and set clear legal boundaries.
- **Enhancing Transparency**: The processes by which AI systems collect and analyze data should be transparent and regularly audited to ensure that individual rights are not violated.

5.3 The Need for Continuous Updates in AI Technologies to Keep up with the Dark Web

Cybercrimes, including human trafficking, evolve rapidly on the dark web, requiring continuous updates to AI technologies. These updates are necessary to keep pace with the technological developments that criminals use to avoid detection.

1. **Adapting to the Evolution of Crimes**:

   Criminals on the dark web continuously develop new methods and advanced tools to evade law enforcement. AI technologies must be updated and retrained periodically to keep up with these developments. For example, more sophisticated cryptocurrencies are now being used, or more complex anonymity techniques.

2. **Advancements in Neural Networks**:

   Deep neural networks used in analysis and prediction must be continuously updated by feeding them new data and improving their learning algorithms. The challenge is that data collected from the dark web is often inconsistent or unstructured, making it difficult to train models effectively (Park et al. 2021).

- **Rapid Response**:

  There is a need for smart tools that can respond quickly to the constant changes in the crime environment on the dark web. AI systems must be capable of automatically adapting to new methods used by criminals, which requires ongoing investment in research and development (Zhang 2023).

Possible Solutions:

- **Continuous Research**: Governments and companies should invest in ongoing research to develop AI technologies that can adapt to changes in criminal behaviors.
- **International Cooperation**: Collaboration between countries to develop shared tools that can be updated in real-time can enhance AI's ability to keep up with cybercrimes.

Artificial Intelligence in Enhancing Law Enforcement and Detecting Sexual Harassment and Child Abuse

Artificial intelligence algorithms have succeeded in detecting words and phrases commonly associated with bullying, filtering out more than two-thirds of threats, insults, and sexual harassment incidents. This new technology relies on deep neural networks to process images and help identify online child sexual abuse materials, which improves the efficiency of detecting such content and reduces exposure to human reviewers. The quick detection of new images also contributes to greater protection of children at risk of sexual abuse.

Many technology companies are now showing increased readiness to utilize AI to detect various types of child abuse content, such as nudity and offensive comments. Google's recent announcement about its commitment to combating child sexual abuse content online reflects cooperation between Google and its partners in fighting online sexual abuse of children.

Third: Mechanisms for Combating Child Sexual Abuse and Removing Terrorist Content on Electronic Platforms

Social media platforms like Facebook have the ability to filter approximately 98% of harmful and explicit content on their platform, thanks to machine learning algorithms. However, there are still shortcomings, particularly when it comes to complex contexts and language translation. This is why machine learning-based innovations, such as **Natural Language Processing (NLP)**, have become very useful in managing user-generated content and improving content moderation.

25 Role of Artificial Neural Networks:

Artificial neural networks simulate human thought processes, such as analyzing words and phrases related to extremism and terrorism. These networks operate in three stages: input, processing, and output, contributing to recognizing negative content and managing it effectively.

26 Natural Language Processing (NLP) to Address Negative and Unethical Communication

NLP allows machines to understand and generate human language, whether written or spoken, improving human–machine communication to resemble human-to-human interaction. This technique enables AI to detect inappropriate, sexual, and unethical meanings across multiple languages.

27 AI Tools and Software Packages

Google launched a software package designed to assist in detecting online child sexual harassment. The package, developed with specialized organizations, uses AI to identify content targeting children at a rate 700% more effective than traditional methods. Google has also developed the **YouTube Kids** app to help parents monitor their children's online activities, providing the ability to block inappropriate channels and set watch times.

Parents can create accounts for up to eight children, monitor content, and even report inappropriate videos. The app is available on Google Play and the App Store for Android and iOS devices.

28 Summary of Key Technological Contributions

- **Deep Neural Networks** are used to identify child sexual abuse materials effectively, reducing exposure to human reviewers.
- **Natural Language Processing (NLP)** helps moderate harmful content, making machine-based decisions about language context and structure.
- **PhotoDNA Technology**, developed by Microsoft, is used by platforms like Facebook to detect and remove known child exploitation images.

29 Conclusion

- **Summarizing the Importance of AI in Combating Human Trafficking on the Dark Web**

  AI has become an essential tool in combating complex cybercrimes, especially human trafficking on the dark web. Through techniques such as encrypted text analysis, pattern recognition, and deep neural networks, law enforcement agencies have been able to uncover and track illegal activities that previously benefited from the high privacy and secrecy offered by the dark web. AI's role in this field not only

enhances the ability to detect suspicious activities but also facilitates collaboration between security agencies globally, leading to significant progress in addressing this transnational crime (BasuMallick 2023).

- **Emphasizing the Need to Continue Developing and Applying Technology**

  Despite the effectiveness of these tools, technical challenges such as encryption and anonymity continue to impede some investigations. Therefore, it is crucial to continue developing the technology, improving algorithms, and enhancing AI's capabilities in dealing with encryption and advanced techniques used on the dark web. Continued innovation in this area will help narrow the gap between the advancements criminals make and the technological capabilities available to combat them.

In conclusion, success in combating human trafficking requires a combination of continuous technological development, extensive international cooperation, and the wise application of available technologies. AI is not just a tool but an essential

Table 1 Challenges and response mechanisms in combating digital sexual exploitation of children on the dark web (Trends & issues in crime and criminal justice No. 711–2025.)

Challenge	Description	Response mechanisms
Deepfake CSAM Production	Use of AI to generate fake child sexual abuse images/ videos that are difficult to verify	Develop AI-based deepfake detection tools; collaborate with major tech companies to trace and analyze data
Anonymity and Concealment	Offenders rely on encryption (Tor, VPN) and cryptocurrencies to avoid detection	Blockchain analysis, tracking financial transactions, strengthening international cybercrime cooperation
Automated Distribution via Bots	AI-driven bots spread illegal content rapidly across multiple platforms	Deploy counter-algorithms to detect abusive bots; enhance early-warning systems for law enforcement
Difficulty in Identifying Real Victims	Mix of real and synthetic material makes it hard to confirm child victims	Create unified international victim databases (e.g., INTERPOL ICSE); combine facial recognition with digital forensics
Legal and Legislative Gaps	Existing laws insufficiently address AI-based crimes and deepfake exploitation	Update legislation to cover emerging technologies; introduce specific laws on deepfake and child digital exploitation
Lack of Expertise and Resources	Shortage of trained professionals in AI-driven digital forensics and law enforcement	Specialized training programs for police and judiciary; partnerships with universities and research centers; funding specialized units

necessity to keep up with modern cybercrimes, and it must remain a focal point for researchers and law enforcement agencies to secure a better and safer future for potential victims (Table 1).

Sources

Second : References in foreign language:

BasuMallick, C. (2023, des 22). *What Is a 6G Network? Definition, Features, and Benefits 6G network enables high-speed, low-latency communication at a pace multiple times faster than fifth-generation networks.* Retrieved from https://www.spiceworks.com/tech/networking/articles/what-is-6g.

Beukema, P. (2024). *Satellite Imagery and AI: A New Era in Ocean Conservation.* from Research to Deployment and Impact.

EU Policy Cycle. (2022). *EMPACTEMPACT.* EU Policy Cycle.

Europol. (2023). *Internet organised crime threat assessment (IOCTA).* Europol. https://www.europol.europa.eu

Gui, S, Song, S, Qin, R, & Tang, Y. (2024). Remote Sensing Object Detection in the Deep Learning Era—. *A Review. Remote Sens, 16*, 327.

https://www.boldbusiness.com. (2024, feb 25). *The Bold Impact of Technology and Artificial Intelligence in Law Enforcement*. Retrieved from https://www.boldbusiness.com/digital/the-bold-impact-of-artificial-intelligence-in-law-enforcement/.

https://humantraffickingfront.org. (2024, mar 25). *The Use of the Internet to Recruit Children by Traffickers.* Retrieved from https://humantraffickingfront.org/the-use-of-the-internet-to-recruit-children-by-traffickers/.

https://syntheticdrugs.unodc.org. (2023, mai 2). https://syntheticdrugs.unodc.org/syntheticdrugs/ar/cybercrime/onlinetrafficking/onlinesalesplatforms.html. Retrieved from https://syntheticdrugs.unodc.org.

https://www.adfsolutions.com. (2024, MAR 31). *Advanced Digital Forensic Solutions.* Retrieved from https://www.adfsolutions.com.

https://www.fastcompany.com. (2024, mar 2). *How AI could help fight human trafficking New detection methods fueled by artificial intelligence could give anti-trafficking efforts a much-needed boost in accuracy and efficiency.* Retrieved from https://www.fastcompany.com/91055657/how-ai-could-help-fight-human-trafficking.

https://www.satcen.europa.eu. (2024, apr 18). *GENERAL CRIME AND SECURITY SURVEILLANCE, European Space Imaging/Digital Globe.* Retrieved from https://www.satcen.europa.eu/services/general_crime_and_security_surveillance.

https://www.satimagingcorp.com. (2024, feb 28). *Artificial Intelligence (AI) and 2D/3D Geospatial Technology-Crime Mapping*. Retrieved from https://www.satimagingcorp.com/applications/artificial-intelligence-ai/.

https://www.socialbakers.com. (2021). https://www.socialbakers.com/blog/21-data-points-for-2021. Retrieved from https://www.socialbakers.com/blog/21-data-points-for-2021.

https://www.space.com. (2024, mar 2). *NASA - Elizabeth Howell, Ben Biggs, Artificial satellites now number in their hundreds of thousands in orbit around Earth,. Retrieved from* https://www.space.com/24839-satellites.html.

https://www.spatialpost.com. (2024, apr 30). *Application of Remote Sensing In Criminology: Enhancing Crime Analysis, ar:. Retrieved from* https://www.spatialpost.com/application-of-remote-sensing-in-criminology/#google_vignette.

https://www.statista.com. (2024a, apr 30). *Human trafficking—Statistics & Facts.* Retrieved from https://www.statista.com/statistics/459637/number-of-victims-identified-related-to-labor-trafficking-worldwide/.

https://www.statista.com. (2024b, apr 21). *Internet and social media users in the world 2024 | Statista.* Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/.

https://www.unodc.org. (2023, July 22). *press-release_-nccpimandtip--unodc--iom-and-ilo-collaborate-to-mark-the-world-day-against-trafficking-in-persons.html*. Retrieved from https://www.unodc.org/romena.

Jafarbiglu, H, & Pourreza, A. (2022). A comprehensive review of remote sensing platforms, sensors, and applications in nut crops. *Comput. Electron. Agric*, 197.

Kobielus, J. (2020). Advancing AI with Neuromorphic Computing platform.

Latonero, M. (2019). Artificial intelligence and human trafficking: A primer. Data & Society Research Institute. https://datasociety.net.

Li, H, Zhu, F, Zheng, X, Liu, M, & Chen, G. (2022). MSCDUNet A Deep Learning Framework for Built-up Area Change Detection Integrating Multispectral, SAR, and VHR Data. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens, 15*, 5163–5176.

Li, X, Du, Z, Huang, Y, & Tan, Z. (2021). A Deep Translation (GAN) Based Change Detection Network for Optical and SAR Remote Sensing Images. *ISPRS J. Photogramm. Remote Sens, 179*, 14–34.

Michailidis, E., & Vouyioukas, D. (2022). A Review on Soft- ware-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones. *Drones.*

MONITORING GLOBAL THREATS. (2012). THE CONTRIBUTION OF SATELLITE TECHNOLOGIES. *Technology and Industry, Version of brochure: 5 November.* Anita Gibson: OECD Directorate for Science.

Number of internet and social media users worldwide. (n.d.).

Park, H.G, Yun, J.P, Kim, M.Y, & Jeong, S.H. (2021). Multichannel Object Detection for Detecting Suspected Trees with Pine Wilt Disease Using Multispectral Drone Imagery. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens*, 14.

Pelton, J., & Madry, S. (2020). *Handbook of Small Satellites- Technology, Design, Manufacture, Applications.* Economics and Regulation.

REPORT OF UN. (2020). *Global Report on Trafficking in Persons.* ONE.

Swihart, J. D., Endert, A., & Brucka, A. (2022). Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective. *Proceedings of the ACM on Human-Computer Interaction, 6*(2).

V. Zelenskyy. (2021). *DECREE OF THE PRESIDENT OF UKRAINE On the National Human Rights Strategy.* Decree of the President of Ukraine.

Zhang, Z. (2023). A Review on Unmanned Aerial Vehicle Remote Sensing: Platforms, Sensors, Data Processing Methods, and Applications. *Submission received*.

From Manipulated Word to Manipulated Algorithm



Katarina Smakic, Nenad Putnik, and Milica Boskovic

When examining numerous ancient states engaged in perpetual warfare, along with social conflicts within class-divided societies, it becomes evident that such conflicts often saw resolution through radical measures, primarily combat between the warring factions. Given that no authority could rely solely on radical measures, methods rooted in religion and tradition were also utilized. These included the maintenance of cults venerating deceased and living rulers and heroes, alongside the application of various propaganda techniques and available resources. The term "propaganda" derives from the Latin "propagare," meaning "to spread," "to propagate," or "to promote." Originally used in the context of disseminating religious doctrines, particularly within the Catholic Church, it referred to efforts aimed at spreading religious truths among non-believers. The term "propaganda" has an interesting and complex history that has evolved over the centuries. Initially, during the seventeenth and eighteenth centuries, "propaganda" had predominantly religious connotations. It was used in the context of spreading religious ideas and teachings, which was particularly important for the Roman Catholic Church as it sought to strengthen and expand its influence. However, it was not until the nineteenth century, especially during the period of the French Revolution, that the term began to be used in a political sense. At that time, it started to denote the systematic efforts of political organizations or governments to influence public opinion by disseminating certain ideas, information, or attitudes to support or promote specific political objectives. The term "propaganda" acquired a negative connotation during the twentieth century, largely due to the negative experiences with propaganda under totalitarian regimes such as Nazi Germany and the Soviet Union.

K. Smakic · M. Boskovic (✉)
Faculty of Diplomacy and Security, Belgrade, Serbia
e-mail: milica.boskovic@fdb.edu.rs

N. Putnik
Faculty of Security Studies, University of Belgrade, Belgrade, Serbia

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2026

H. N. El Shenraky (ed.), *Analytical Studies on Cybercrimes Against Children in the Dark Web*, https://doi.org/10.1007/978-981-95-8469-7_12

Today, the term "propaganda" is predominantly used to refer to manipulative or biased efforts to shape public opinion, often with the goal of promoting specific political or ideological interests. As Slavujević (1997:19) notes, "The religious frameworks governing the entirety of social life, and particularly the emphasized role of religion in legitimizing and reproducing systems of power and social relations in ancient states, determine the forms in which propaganda appears. This continues until, in the later development of certain states, particularly in Greece and Rome, politics and propaganda become secularized and begin to emerge in a pure form as relatively independent entities."

In ancient states, as Slavujević (1997) highlights, the first form of political propaganda involved emphasizing the political roles of religion by highlighting religious elements that represented the ideology of power. This approach simultaneously exercised social control and directed the political goals of propaganda using non-philosophical elements. This form of propaganda was manifested through the promotion of deities, the establishment of order between the cosmos and the state, the actions of "higher powers," and similar concepts. Propaganda was directed at the masses, whose psychology, or crowd psychology, significantly differs from the psychology of an individual participating in that crowd. As le Bon (1989) notes, "[…] thousands of separate individuals can at certain moments, under the influence of certain strong emotions, as is the case in a major public event, acquire the characteristics of a psychological crowd. Under certain conditions, even half a dozen people can form a psychological crowd, while hundreds of people who have gathered by chance may not. On the other hand, an entire nation can, under the influence of certain factors, become a crowd without any visible aggregation" (p. 10).

A clearly expressed "propaganda intent" can be observed from the very beginnings of civilization. From the earliest actors in ancient states and political events, rulers have openly intended to influence the attitudes and behaviors of individuals and social groups through their actions. The general conclusion is that successful propaganda is one that manages to align cognitive and affective elements. Neither of these two approaches is inherently more effective, nor does either unconditionally protect against manipulation: using objective logic in propaganda does not guarantee the acceptability or truthfulness of the messages, and using "affective logic" does not necessarily imply manipulation. It is natural for people to resist change and, therefore, to defend their attitudes when confronted with differing opinions and beliefs. Attitudes have an emotional component, and propagandists can influence desired behavior by exploring and understanding these attitudes.

In the modern context, we can refer to the views of Edward L. Bernays, known as the father of modern propaganda, regarding its role in democratic societies. Bernays argued that propaganda is inevitable in the modern age because, without the organization and manipulation of the masses, there would be general chaos and confusion.

In his book "Propaganda" (1928), Bernays explains the structure of the mechanism that controls public opinion and discusses how everything is manipulated by a special advocate who seeks public approval for an idea or object. Bernays describes this through various spheres of society, such as the economy, political leadership,

education, public services, art, and science. He argues that the introduction of propaganda into the modern democratic framework of society is inevitable but emphasizes the importance of constantly preventing its abuse. Bernays also highlights the significance of the invention of the steam engine, the printing press, and the opening of public schools as the trinity of the Industrial Revolution, which strengthened the role of the citizenry in the decision-making process. Louis Althusser proposed the thesis that the educational ideological apparatus is the state ideological apparatus placed in a dominant position in mature capitalist social formations as a result of violent and ideological class struggle against the old dominant state ideological apparatus.

Louis Althusser explained his thesis by emphasizing that all state ideological apparatuses, despite their differences, ultimately achieve the same goal: the reproduction of productive relations, namely capitalist relations of exploitation. According to Althusser, education is not neutral but functions as an ideological apparatus that serves to reproduce social norms, values, and power relations. In capitalist society, the educational system plays a crucial role in maintaining capitalist relations of exploitation by shaping people's attitudes, beliefs, and behaviors according to the needs of the capitalist system. Althusser extensively researched how capitalist ideology is transmitted through education, highlighting the role of teachers as bearers of ideology and propagators of the capitalist order. He also emphasized that education is not merely the transmission of knowledge but a means of controlling and reproducing social structures, including the exploitation of the workforce in the capitalist system.

Similarly, Bernays argues that teachers must act as both educators and propagandists, and that every social group occupying a particular position also accepts an ideology that aligns with their role in class society, whether as the exploited, exploiters, enforcers of repression, or professional ideologists.

In a democratic society, individuals are considered free, and this freedom is enabled by access to information and media that make society transparent. Democratic societies are characterized by open communication, assuming that people can recognize manipulations. However, claiming that manipulation, propaganda, and disinformation are relics of the past risks falling into a trap. It raises the question of whether democratic society is truly resilient to such phenomena. This notion assumes that the audience can identify complex language patterns and manipulative discourses, implying that such content cannot be considered real manipulation because the audience can immediately interpret it. Yet, believing that we are immune to such content is the first step in manipulation itself. It suggests that our choices and opinions are independent, implying that we are entirely free in making decisions and drawing conclusions. In the digital age, our resilience to manipulation depends on several factors, including levels of education, critical thinking skills, media literacy, and awareness of manipulation techniques.

However, in the modern digital environment, manipulation can be very subtle and sophisticated, making it challenging to recognize and avoid its effects. Studies on the technology used to alter human behavior patterns began in 1997 as a new field of research, and scientists agreed to name it "captology" (Computers As Persuasive Technologies). Fogg defined computer systems that change user behavior patterns as "computer systems, devices, or applications intentionally designed to influence

attitudes or behaviors of users in specific ways" (Fogg, 1999). This formulation emphasizes the intention of the creators as a crucial factor in the use of these technologies, where the technology itself does not inherently persuade, but its creators intend to use it to influence human behavior patterns.

Fogg suggests that captology leverages existing persuasion theories from fields such as psychology, communication, and media because they have an empirical basis that allows for predicting effects, thereby leading to implementation in captology. The strategies used in modern technologies to persuade users have already been applied in traditional media but have now taken precedence in contemporary technologies. "In the digital world, we encounter persuasion attempts with every click, and practically every website aims to persuade: creators try to influence users' attitudes or behaviors in some way, whether it's signing up for a service, sharing video content with friends, or entering an email address."[1] Designers and programmers who embrace persuasive strategies and implement them in their applications are aware of their effects on users and should certainly consider ethical considerations. Carey Heckman et al. (2000) focused on ethical issues in the application of these technologies and proposed that all creators of such content assess whether the persuasive strategies they use genuinely benefit users and ensure that users are the ultimate beneficiaries of such technologies.

Ethical design principles for new technologies proposed for adoption by all web content designers include the following: persuasion must never be unethical; creators must take responsibility for what may happen to the user; they should respect user privacy and not share personal information with third parties; they must clearly express their intentions, methods, and expected outcomes; they must not deceive users to achieve desired results; and they must follow the "golden rule"—never persuade users to do something they themselves would not accept.

People often treat new technologies as self-aware: for example, frustration when paper gets stuck in a printer or when a computer stops responding, which leads to emotional reactions manifested in direct interactions with machines, whereas technologies are merely channels transmitting what content creators want us to see or encouraging users to act in certain ways through persuasive strategies.

Tools of captology are recognized as cognitive biases (such as risk aversion when time is limited, driven by a strong message), as persuasion weapons (utilizing "scarcity principle" and "authority theory"), and leveraging productive laziness (factually grounded that people sometimes skip certain preferences or read carelessly), along with decision fatigue (related to user exhaustion through excessive exposure to choices that provoke the path of least resistance). The authors of the aforementioned study raise the question of whether the human brain can evolve and learn if these tools become uniform and inevitable parts of everyday life. They emphasize that artificial intelligence, a field within computer science, includes one of its primary components called expert systems, which are depicted as databases, knowledge bases, and reasoning mechanisms. Artificial intelligence simulates human intelligence processes using machines, especially computer systems, while specific

[1] http://captology.stanford.edu/resources/article-new-rules-of-persuasion.html.

applications of AI include expert systems, natural language processing, speech recognition, and machine vision.

This area of computer science is often paralleled with human intelligence and intuition because its knowledge base relies on symbolic representation and bears similarity to human intelligence. Additionally, artificial intelligence (AI) is a key characteristic of transhumanism, accompanied by the concept of "digital manipulation." One example of digital manipulation is deepfake technology, which utilizes artificial intelligence (AI) to create false yet convincing audio or video recordings. This technology enables the creation of videos where it appears that a person is saying or doing something they have not actually said or done. For instance, a deepfake video may depict a political leader saying something controversial or inappropriate, even though they never uttered those words. When such fake recordings are shared on social media or in the media, they can cause significant confusion, misinformation, or even influence political elections or an individual's reputation. Deepfake technology can also be used in the context of online fraud, where it is employed to falsely represent legitimate business executives or other authorities with the aim of gaining money or accessing confidential information.

This technology can be very dangerous because many people find it difficult to recognize as manipulation, especially if they are unaware of the existence and prevalence of such techniques. Another common example of digital manipulation is microtargeting in political campaigns. Microtargeting uses data collected about users to tailor political messages to specific demographic groups or even individuals. This practice may involve analyzing social media behavior, search history, content likes and shares, as well as other personal data to create a user profile. For example, a political campaign might use this data to determine which issues are most important to a particular person or group and then adjust messages to align with the interests of these targeted groups. This can lead to a situation where different groups receive completely different messages from the same candidate, creating a fragmented and polarized environment.

Manipulation of algorithms in social media is another example, where this type of manipulation uses algorithms to determine what users will see in their feeds to increase the visibility of certain content or decrease the visibility of others. For instance, popular content creators or political organizations may employ various techniques such as coordinated campaigns of liking, commenting, and sharing to "game" the algorithms and enhance the visibility of their messages. This can lead to a distorted perception of reality, as users may feel that a majority supports certain views when it is merely a result of algorithm manipulation. Algorithm manipulation involves using techniques or strategies to influence how algorithms display or rank content, typically aimed at increasing the visibility or popularity of specific information, individuals, or products. It starts with a complex understanding of how the algorithm operates.

Algorithms on social media and search engines often use complex criteria to rank content, including likes, shares, comments, time spent on content, language used, keywords, and other engagement indicators. One common technique is generating fake engagement to "trick" the algorithm into thinking that the content is highly

popular. This can involve the use of bots, fake accounts, or paid individuals who artificially like, comment, or share specific content in large numbers. The more engagement the algorithm detects, the higher the chance that the content will be shown to more users. Therefore, groups or organizations sometimes conduct coordinated campaigns to increase the visibility of their content or viewpoints. These campaigns may include synchronized sharing, commenting, and liking of content at specific times, signaling to the algorithm that the content is "trending." Another manipulation tactic is using popular or viral keywords to increase the likelihood of content being noticed. This can include using clickbait headlines or adding popular hashtags that may not be directly related to the actual content but serve to attract the algorithm's attention. Organizations or individuals may attempt to influence algorithms by avoiding certain words or topics that algorithms might perceive as problematic, or by favoring those considered positive or popular. An example of manipulated algorithms can be seen when a group or individual employs strategies to deceive social media algorithms to increase the visibility of their content or control narratives. One of the most well-known examples is the case of Russian interference in the 2016 US elections, where groups like the Internet Research Agency (IRA)[2] used various tactics to manipulate social media algorithms and spread disinformation. The IRA created fake accounts on platforms such as Facebook, Twitter, and Instagram, using them to share controversial or polarizing content often focused on political and social issues. Their goal was to increase user engagement, signaling to algorithms that the content was popular and worthy of promotion. They employed coordinated sharing of content, creating a network of fake accounts that would share and like content in a synchronized manner to boost its popularity.

When algorithms recognize high levels of engagement, they often increase the visibility of that content, thereby amplifying its impact. They have used headlines and images designed to provoke strong emotions such as anger, fear, or excitement to attract more clicks and shares. Algorithms often favor content that evokes emotions and boosts user engagement. IRA utilized microtargeting techniques to direct their messages toward specific demographic groups, using data about users and their interests. This enabled them to manipulate algorithms so that content reached the most vulnerable and susceptible users. The result of this manipulation was the spread of misinformation, polarization of public opinion, and erosion of trust in institutions and media. This example illustrates how algorithms can be manipulated through coordinated campaigns, fake accounts, and deceptive content, underscoring the need for increased supervision, transparency, and accountability in the design and implementation of algorithms on social media and other digital platforms.

One of the key techniques these algorithms use is recommending content based on users' past behavior, preferences, and data collected from other users with similar profiles. Algorithms may show users only content that aligns with their previous interests or views, creating "filter bubbles." This can manipulate user behavior by enclosing them in a space where their views are only reinforced, leading to increased

[2] The IRA and Political Polarization in the United States, University of Oxford, https://demtech.oii.ox.ac.uk/research/posts/the-ira-and-political-polarization-in-the-united-states/.

polarization and reduced diversity of thought. Algorithms are often designed to be highly engaging and elicit a sense of satisfaction, aiming to keep users on the platform for as long as possible. This is achieved through personalized notifications, reminders, and visual stimuli that encourage users to return more frequently and stay longer. This approach can create dependency on social media and alter behavior patterns.

Algorithms often favor content that has already gone viral or elicits strong emotional reactions. This strategy can manipulate user behavior by guiding them toward specific content, and in some cases, promoting the spread of misinformation or controversial topics that provoke strong reactions. Social media platforms use algorithms to encourage user interaction with content, and these algorithms can manipulate user behavior by prioritizing content that encourages interaction, even if the content is controversial or misleading. These examples demonstrate how algorithms can be designed to control and influence user behavior, often aiming to increase engagement and time spent on the platform. This raises important ethical and responsibility questions in the design and implementation of algorithms that have the power to shape human behavior in such subtle ways.

Algorithms designed in this way can also influence biological changes within the body, particularly through stimulation of the brain's dopamine system. The dopamine system plays a crucial role in processes of reward, motivation, and pleasure.

Dopamine is a neurotransmitter released in the brain in response to pleasant or rewarding activities, such as eating delicious food, listening to music, or successfully completing a task. Algorithms that use personalized notifications, reactions, and other incentives can trigger dopamine release, creating a sense of pleasure and reward. This effect can motivate users to return and spend more time on the platform because when a user experiences pleasure through interaction with online content, that experience can become habitual. Algorithms designed to provide continuous stimuli can encourage users to develop behavioral patterns that rely on dopamine stimulation, which can lead to increased platform use. Long-term and frequent exposure to content that triggers dopamine spikes can lead to addiction.

Users who become addicted to social media or other online platforms may feel the need to constantly check their profiles, react to notifications, or seek new stimuli, even when it negatively affects their daily functioning. Some social networks and most video games use a technique called "variable ratio reinforcement," where users do not know exactly when they will receive a reward (like new likes, comments, messages, etc.). This principle is utilized in slot machines and can induce a stronger addiction effect because unpredictability increases the intensity of anticipation and engagement. Such an embedded algorithm simulates a reward system where the user receives a random reward each time they participate in a particular activity. This principle of variable reward is known for causing an increase in dopamine because the user does not know exactly when and what reward they will receive, which encourages repetition of the activity and increases engagement. This type of reward system is often used in games, social media applications, and even learning applications, as it motivates users to continue using the platform and return for new rewards. However, this approach can also lead to addiction and physical changes in the brain, particularly in the gray matter, where changes in volume may reflect adaptive brain plasticity in

response to frequent stimulation. This could suggest that frequent video game playing or similar activities that engage the reward system may lead to structural changes in the brain. These changes may indicate greater stimulation of the reward system, often associated with experiences that induce pleasure or excitement. In the context of video games, this could mean that frequent playing can enhance the activation of the reward system (Kühn, Romanowski, Schilling, 2011). Such profiling can be abused by encoding algorithms that target specific groups (children and youth) and use them for malicious contact with the intention of deception, exploitation, or other illegal activities. This may include grooming (a process where malicious individuals build trust with children online to sexually exploit or abuse them in other ways), phishing and social engineering, and impersonation (creating false identities to manipulate or lure them into actions that may be dangerous or illegal). The infiltration of technology into all aspects of life and work has resulted in children being born surrounded by digital tools and technology at every new step they take.

At a very early age, while they are still intellectually and emotionally immature, children interact with technology and accompanying applications, primarily social media. Although the age limit for active use of certain applications is set at 13 years, this does not prevent children from bypassing these restrictions. Children are present on social media; in the UK, 21% of those aged 8–11 years and 4% of those aged 5–7 years have a social media profile (OFCOM, 2019). We witness how adults often fall victim to serious manipulations and scams in cyberspace, and we cannot even begin to grasp the full scope of threats facing children using these applications. Due to their insufficiently developed emotional and social intelligence, knowledge, and awareness of dangers, children engage much more naively and recklessly on social media, participating in various interactions. Considering that children have even less social experience to understand social appropriateness and audience interpretation of disclosures, they may be even more likely to share inappropriate information online (Christofides et al., 2011), but also to receive it. In addition to the obvious security risks, attention must also be drawn to the psychological and emotional consequences that may arise for children due to exposure to various content and conversations. A large number of social interactions in the cyber world can create a distorted image for children regarding their popularity and importance, which, in the real world, can lead to frustration, dissatisfaction, withdrawal, or aggression. Manipulators and criminals consciously exploit children's basic needs for belonging, protection, and love in cyber interactions with young people, with the ultimate goal of blackmailing them or turning them into victims of pedophilia and/or human trafficking.

Message manipulation is not something "reserved" only for the child population—techniques of fake news and shaping public awareness have been known and applied for decades. Fake news and disinformation are very carefully crafted, utilizing psychological insights into how people cognitively and emotionally react to specific information. Disinformation works through a series of cognitive hooks that make the information appealing, triggering a psychological reaction in the reader (Ruffo et al., 2023). Manipulative information and fake news are created to be attractive, easier to understand, and provide message at mode capable for further spreading and repeating. What is important, manipulative information is created to trigger

emotions. Driven by emotions, we find it more difficult to discern what is right or wrong, true or false. The opportunity that today's media provides to creators of misinformation is the ability to exert an almost constant influence—"repetition is a well known propaganda mechanism, and it is exploited by social media filtering algorithms that decide what content deliver to whom, by including the users' taste, evetually building a reinforcement feedback loop on users' walls" (Ruffo et al., 2023). Moreover, when an algorithm recognizes a message sent by a "trusted" contact/friend that also contains a certain opinion, the effect of repetition and spreading influence only grows, acting like an echo to everyone connected to the network. The repetition of information has long been shown and proven to be the best way to influence the awareness and thinking (and consequently behavior) of the end user, i.e., the target of manipulation—thus creating a bubble of illusory truth. This process often occurs outside the user's will and is based on personalization and the collection of as much information as possible about the individual or group being targeted. Profiling involves recognizing patterns and matrices of behavior, opinions, posts, and habits, which are then categorized into defined categories, stereotypes, and compatible generalizations. Personalized profiling aims to define the selected individual according to pre-created categories and thus expand the circle of group targets. As such, personalization paradoxically, denies individual uniqueness through a "smart" homogenization that negotiates the diversity of humankind (Yeung, 2018). Thus, the individual is significant only until they are "acquainted with" and placed into a psychologically and sociologically defined group, upon which manipulative tactics are applied. This method is commonly used in political propaganda and marketing to enhance consumerism. However, when discussing children interacting on social media, malicious algorithms and influencing thoughts are far more dangerous to their health and lives. Algorithms can even operate autonomously once created, assessing individuals based on their reactions, akin to the "reward and punishment" method used in early childhood education. For example, they can use A7B testing to experiment with various messages until they find the version that best exploits individuals' vulnerabilities (Calo, 2013:996).

Manipulation has become much easier with the development of so-called affective computing or emotional AI, which largely relies on captology—a comprehensive set of knowledge about using persuasive technology for the purpose of confusing, deceiving, and controlling thoughts. In its most malicious form, persuasive techniques can seriously undermine someone's self-control, independent thinking, and decision-making. These can indeed stimulate users in a powerfully subconscious and hormonal way (Reviglio and Agosti, 2020). Malicious algorithms embedded within the structure of social networks design the network architecture, environment, and virtual infrastructure through which they operate toward the user or group of users. This is the so-called "architecture of choices," which in reality does not leave the user with a choice but manipulates them into actions desired by the malicious attacker. Ultimately, this choice architecture shapes what content the user will receive, what will be presented and recommended to them, and how they will react to it. The way it is delivered is determined by design—is it scrolling feed, srory, reel, forum, etc. (5Rights Foundation, 2021). Malicious algorithms rely on numerous studies and

knowledge about ways to present content, including its appearance, accompanying sounds, color schemes, message duration (TikTok), or the number of characters needed to express something—simultaneously, effectively, and without restrictions on a specific word choice or sentence length (X, former Twitter). "Frameworks such as BJ Fogg's B = MAP demonstrate how these approaches are used to steer user experience design (US Design). Designers aim to tap into user's underlying motivations, make the experience as seamless and natural as possible and provide regular prompts or triggers to build behaviors into habits" (5Rights Foundation, 2021:26). "Dark patterns" employ persuasive techniques and captology in the most dangerous and malicious ways to influence the user and modify their behavior in favor of the attacker's interests. In this scenario, individuals, particularly children, become victims of perfidious psychological and emotional abuse, which can lead to very serious consequences for their integrity and even their lives. Children and young people can unknowingly and automatically be "drawn into" their virtual life guided by malicious algorithms, whose ultimate goals are set by the creator of such cyber infrastructure or those who commissioned it for their purposes.

Today, when we talk about the dangers children face in cyberspace, we are no longer just referring to manipulation for purchasing specific products or bullying. Rather, we are addressing the widespread manipulation aimed at obtaining explicit content from children, which can escalate to coercing victims into engaging in chat sessions, live streaming, meetings, and eventually subjecting them to sexual abuse. Data collection techniques have become so sophisticated that marketers, advertisers, and even politicians are increasingly adept at predicting preferences of individuals, including children, even before they themselves have consciously considered their choices (Fourie, 2020:245).

Social media, with their construction, appearance, and interactive capabilities, are highly attractive and accessible to children. However, insufficient knowledge and unawareness about the potentially malicious architecture and behaviorally designed algorithms behind these applications can expose children to dangers over time and lead to serious disorders such as depression, social anxiety, or emotional instability (Ahlawat and Anand, 2022:12). Persuasive technology fundamentally aims to change behavior and influence thought processes through technology—enticing content that increasingly keeps children engaged on social media, often at the expense of sleep, concentration, and cognitive function, becomes a dangerous tool in the hands of individual predators and organized criminal groups, who often carry out their intentions through the so-called dark web.

Modification of thoughts and behaviors using captology and malicious architecture based on the so-called Big Data-driven behavior system is also referred to as "hyper-nudging," a process through which an individual begins to form opinions under strong external influence, in this case, predators using technology. Hyper-nudging, opposing personal integrity and autonomy, through constant influence of malicious algorithms, is indeed the "invisible hand" of behavioral prediction and modification (Zuboff, 2015). Techniques like these addictive techniques, with a definite intention and steps toward the complete victimization of a child, can first lead them into depression, conflict with parents and authorities, and subsequently,

with such isolation and social anxiety, easily introduce them into the world of "false love"—pedophilia and trafficking. Innovative new technologies, such as cripto currencies are unfortunately powering the Dark web with its harmful child content and streaming of child sexual abuse, while making it increasingly difficult for law enforcement to stay abreast (Fourie, 2022:233).

In the fight against such abuses, the focus often turns to educating parents and children to prevent and raise awareness about threats lurking in the digital environment. The term promoted in this domain as part of education is media literacy. Numerous definitions of media literacy target various aspects within the media literacy space, from its basic concept—individuals' ability to create and understand media content—to the meta-language of media itself and critical reflection on its content. The question for establishing a clearly defined concept of media literacy lies within specific abilities to create media content, interpret it, and subsequently engage in critical thinking. What is common to all definitions of media literacy?

A large number of studies have been conducted on the topic of clearly defining media literacy, including analyses of definitions aimed at reaching this understanding. James Potter's research (Potter, 2022) uncovered more than 400 elements that constitute definitions of media literacy. These elements are organized into a framework comprising six categories, which cover the entire spectrum of perspectives given for defining media literacy over the past decades in works published in the Journal of Media Literacy.[3] Sonia Livingstone, in her definition of media literacy, includes all of the above except that her definition applies to both traditional and digital media. She states that her definition of media literacy is "the ability to access, analyze, evaluate, and create messages across a variety of contexts" (Livingstone, 2004). In the 1970s, a large number of authors provided definitions of media literacy. For example, Beentjes, Konig, and Rozenbaum (Rosenbaum et al., 2008) analyzed definitions of media literacy in various scientific papers and books, starting from the premise that media literacy involves two key concepts: media production and media use.

Their basic hypothesis was that media influence how authors create their media content and what that content will be, while at the same time, media also influence end-users who provide feedback on the type of product/content they desire. From the above, we can see that the producer-media-user relationship is a two-way communication, and media content creators could predict suitable content based on user feedback. The assertion of these authors stemmed from the influence process, which they translated into four categories of knowledge they termed dimensions. Each dimension focused on studying the interrelationship between producer-media-user, as well as the relationships within the environment of each.

Under the first dimension, the authors established a category for organizing knowledge on how media influence the ideas of producers in media production, while the second contained ideas on how stakeholders construct media content due to influences from cultural, economic, and political contexts. The third dimension contained ideas on how media influence users collectively and individually, and the fourth dimension

[3] Journal of Media Literacy Education. The official publication of the National Association for Media Literacy Educaton (NAMLE). www.jmle.org.

dealt with knowledge on how people handle and understand media. Hans Martens suggests that there are many proposals for the definition of media literacy, and despite the multitude and diversity of their meanings, there is enough consensus that "[…] fundamentally, media literacy depends on knowledge and skills. Specifically, individuals should acquire knowledge about key aspects of mass media phenomena, such as media industries, media messages, media audiences, and media effects" (Martens, 2010). The author argues that this is primarily necessary as protection against potentially negative effects, and also for people to use mass media more self-consciously and make decisions that can improve their lives in general. Being immune to manipulation involves constantly educating oneself, that is, the individual's initiative to make their life a constant process of self-education, thereby acquiring the skills and knowledge that enable them to be thinking beings is another concept in the definition of media literacy among many others. No matter how many elements the definition of media literacy includes, it is based on the relationship between producer-media-user, but in the age of digital technologies, that relationship has changed significantly, with most people unaware of such changes. Manipulation has taken on a completely new form and uses computer algorithms as technology for persuasion. Therefore, whether the user's choice is their own, conditioned by media messages, or whether the user has been psychologically altered so that their response aligns with what the computer software intended, remains a critical question.

Understanding the significance of interactive technologies and their influence on changing audience opinions, attitudes, and values, as well as their impact on behavior change and the reliability of predicting it, is more important today than mere contemplation of the definition of media literacy. While researchers debate what should be included in the definition of media literacy, a completely different kind of spectacle unfolds in the digital sphere, often without anyone fully grasping its true significance. Research into persuasive techniques dates back to ancient Greece, from the sophists who taught rhetoric and eristic, to Aristotle who studied rhetoric as the art of determining the means of persuasion in a given situation (Fogg, 2002:62).

The ancient Greeks believed that public speaking significantly influenced the audience, with privileged members of Greek society learning skills in public speaking to sway opinions or motivate listeners. They considered the art of public speaking crucial to maintaining a healthy democracy (Fogg, 2002:63). These rules were defined by various laws and regulations, but the essence of captology is to influence the human psyche by evoking emotions, instinctive actions, and the use of symbols—all elements of pathos, ethos, and logos—now enhanced by the relationship people have developed with computers and the vague notion that they are protected in the digital sphere. As Divna Vuksanović points out, "the contemporary cave expands and is designed not according to human measure, but to the technology that ensures profit. Any abstraction, aimed at separating these phenomena, unless critically questioned about the entire system of mediation, becomes superfluous, as it supports the artificial construction of the real, existing in an aesthetic way, solely for the reproduction of the capitalist world" (Vuksanovic, 2020).

The evolution of computer technology, from its early days as data processing tools to the widespread adoption of the internet for social interaction, has been pivotal.

Initially synonymous with freedom of speech and expression, the internet empowered individuals to create content without institutional approval. However, over time, digital platforms and social media have institutionalized this space, integrating commerce, education, entertainment, and social interaction. This shift became especially pronounced during the COVID-19 pandemic, making online presence nearly obligatory and smartphones indispensable in daily life.

Shoshana Zuboff introduced the term "surveillance capitalism" to describe how corporate interests shape the digital world using algorithms and technologies to control and manipulate information. She poses the question of whether we will all work for smart machines or if smart people will manage these machines. Zuboff highlights that currently, 3 billion people use information and communication technology systems out of a global population of 7 billion, defining surveillance capitalism as "the unilateral claim to human experience as a free raw material for behavioral data production. Where industrial capitalism transformed natural resources into commodities, surveillance capitalism claims human nature as a new marketable commodity, profiting from markets of future behavior" (Perisic, 2021).

In such an environment, establishing regulations to protect the most vulnerable groups in our society, especially the youth, becomes crucial, given the prevalence of virtual reality without adequate defense mechanisms. Clearly defining the dominant ideology is essential for setting a legal framework that aligns with the values pursued by that ideology and for sincerely recognizing the threats posed, which can only be identified through specific ideologies. Surveillance capitalism and the dominant ideology, particularly within neoliberalism, have a mutually reinforcing relationship. Neoliberalism fosters an environment that enables and encourages practices of surveillance capitalism, while surveillance capitalism utilizes neoliberal principles of free markets, privatization, and deregulation to justify its business models and practices.

In a neoliberal environment, the concept of freedom of speech is often invoked to justify practices of surveillance capitalism. Companies like Google and Facebook frequently cite freedom of expression and the First Amendment to justify their practices and evade regulation. Cyber-libertarianism, which advocates for minimal regulation in the digital world, is also compatible with the ideology of surveillance capitalism. Neoliberalism favors an economy based on innovation, technology, and digitalization, which provides fertile ground for surveillance capitalism as it utilizes cutting-edge technologies for data collection and analysis, thereby creating new opportunities for profit. In the face of these challenges, it is crucial to recognize the dangers ahead and establish regulatory mechanisms that can protect the most vulnerable groups, especially the youth.

The development of a world dependent on technology, both socially and in other aspects, has made it nearly impossible to function in modern society without using these technologies. Attempts to resist the influence of persuasive technologies often result in social isolation. Raising awareness or implementing legal regulations to limit the impact of persuasive technologies could reduce their power over freedom of choice and thought in the use of modern technologies. However, the strength of the capitalist machinery, which uses these tools to increase profit, currently outweighs

the power of individuals who understand how they operate. This unequal power dynamic complicates the fight against manipulation and control arising from the use of these technologies.

Despite the challenges, recognizing and highlighting such threats, establishing legal and regulatory frameworks, and disseminating information about potential dangers can be a first step toward reducing the influence that capitalist systems exert through technologies and persuasive tools. In this complex environment, understanding the economic, political, and socio-cultural aspects of each message becomes exceptionally difficult. Additional challenges arise from specific tools designed to influence unconscious processes in people, aiming to shape their reactions, behaviors, and attitudes. This type of manipulation leads us into the ambiguous realm of a potential transhumanistic society, where the boundaries between human and technological intelligence have become blurred. This situation raises the question of how to preserve traditional values that have always been the foundation of human civilization, while simultaneously paving the way for new forms of interaction and evolution. Keptological tools, when used within democratic systems, create serious dilemmas regarding transparency and the reliability of information. Data manipulation and precise message targeting through these tools can significantly influence political processes, casting doubt on the authenticity of public opinion. This digital paradigm, combined with sophisticated techniques for influencing the unconscious, poses a serious threat to democratic principles. The development of regulatory frameworks and technological solutions, along with public education and awareness, becomes crucial for preserving the integrity of democratic systems in an era of pervasive digital manipulation. Investing in innovation and technological advancement is often justified by the benefits to humanity and the efficiency in performing every life or work function. However, this sometimes aggressive promotion of the benefits of AI and other technologies by scientists can create a kind of moral vacuum or even a stagnation in moral deliberation, portraying those who seek to ethically and legally regulate these areas and cyberspace as hindrances to progress and opponents of freedom of thought.

Whenever science or simply humans reach a point where finding exact answers isn't easy—and further AI development is one of such dilemmas—we turn to philosophy, ontology, the root of everything, through a reconsideration of our place not only on this planet, but in the entire universe. In those moments, it is important to remind ourselves of the fundamental values on which everything is built. The question arises whether ancient thinkers and the first creators of legal systems in the world would be happy to entrust AI with gradually acquiring the things that make us Human—learning, consciousness, critical thinking, and reasoning. However, not a small number of scientists, and even post-modern philosophers, seem to have been successful in usurping and managing the issue of ethics and rights from their point of view. This significant group of influential researchers and thinkers calls themselves transhumanists, and the idea of Transhumanism itself originated in 1927. Then the evolutionary theorist Julian Huxley defined transhumanism as "the belief that human beings need and must transcend themselves, realizing new possibilities for human nature" (Hauskeller, 2012:39). Transhumanism, we can also use that term—preaches

the use of all technological possibilities to overcome the natural and biological limitations of life and existence. Transhumanism wants to do something against the terrifying fact of mortality (More, 1996).

Almost guaranteeing achieving longevity, "cheating death" and aging, and creating beings immune to all diseases, transhumanists advocate for unquestionable and enormous influence and use of nanotechnology, biotechnology, and all other technological and information disciplines, for the purpose of creating posthumans—lifelong and perpetually satisfied inhabitants of the planet. Even a group of scientists from the United States, together with the government, created a report in 2002 titled "Converging technologies for improving Human Performance," in which it is stated that the expectations of the U.S. National Science Foundation and Department of Commerce are so serious that "nanotechnology, biotechnology, information technology, and cognitive science will soon be able to solve all the world's problems" (Hauskeller, 2012:40).

Such a nonchalant attitude toward the unquestionable and almost obligatory integration of technology with human characteristics, particularly among many practitioners in psychology, security, and law, should raise alarms. The enhancement of cognitive abilities not through methods and methodologies of learning, knowledge transfer, and memory improvement, but rather through waves, signals, and algorithms emitted by (micro)technology, raises concerns not only from a common sense and ethical perspective but also from a security standpoint.

Considering all that has been said about modern technologies, surveillance tools, captological tools and malicious algorithms, without hesitation we can pose questions: will this only create happy and cognitively superior beings, or also a legion of obedient followers, manipulated individuals, and those with directed pathological behaviors? Can we trust the noble intentions of these modern, or post-modern philosophers and scientists, or is justified suspicion that they can create soldiers devoid of fear eager to kill, consumers unaware of whether they truly need certain products, children who won't understand what healthy attention, love, and protection mean versus pedophilia and sexual abuse? These questions arise in various legal, ethical, and artistic circles.

Agamben (1998) explored the dangers of technology misuse in the realm of biopolitical control and repression, while in certain literary works by Salvador Sanza, the dark side of transhumanism is depicted, where the pursuit of perfectionism leads to monstrosity and violence (King and Page, 2017:24). What transhumanists present as a world surpassing even Thomas More's Utopia in terms of being better, if viewed from ethical and security perspectives, is actually a dystopia. The superior human is essentially a servant—a body used by programmed technology, healthy and immortal in its service to the principles of consumerism, manipulation, and abuse. Nature does not need immortality, as it has its own structured chemical, physical, and biological processes and a clear food chain, of which humans are just one part.

Transhumanism is a dystopia because it undermines all the laws and regularities created by nature's work, which have sustained us and the Planet for thousands of years. This can result in environmental apocalypse and societal collapse (King and Page, 2017:26). As Fukuyama (2004) emphasized, transhumanism undermines

basic human rights; creating perfect beings without differences in intelligence, abilities, or appearance erases awareness of diversity, challenges, empathy, and development. "If we begin to transform ourselves into something superior, what rights will these enhanced beings demand and possess compared to those who once existed?" (Fukuyama, 2004:42).

Transhumanists aspire, at least narratively, to create superhumans who will not know sadness, pain, ignorance, illness, or death. The focus of improvement is on the individual, not the societal system that may have exerted pressure on individuals that transhumanists seek to control (Sand and Jongsma, 2016:292). Transhumanism does not address the weaknesses of certain political regimes, nor does it critique autocracy, ruthless market competition, or the existence of classes, hunger, and societal marginalization worldwide. Without clear criticism of the socio-economic and political state of the world, transhumanism merely presents an ideology of imagined utopia, where creating the superhuman solves everything. Consequently, we see how this post-philosophy, despite scientific efforts, lacks essential substance and is focused on mastering human thoughts and bodies, with technology as a mandatory tool. Therefore, perhaps it is not surprising that many cyber threats and the creation of malicious algorithms remain unresolved legally and criminally, and that manipulators and predators are always a step ahead of internet protection measures on the Deep and Dark Web. The loud promotion of transhumanism through scientific papers and government reports in various countries indicates that the legal, sociological, and security struggle against this ideology is not utopian but dystopian—facing numerous obstacles.

References

Agamben, G. (1998). *Homo sacer: Sovereign power and bare life*. Stanford University Press.

Ahlawat, K., & Anand, D. (2022). Misuse of persuasive Technology in Social Media with Subsequent Solutions. International Journal of Multidisciplinary Innovative Research, 2(4), 11–24.

Bernays, E. (1928). Propaganda. Retrieved December 10, 2023, from https://www.voltairenet.org/IMG/pdf/Bernays_Propaganda_in_english_.pdf.

Calo, R. (2013). Digital Market Manipulation. George Washington Law Review, 82, 995–1051.

Christofides, E., et al. (2011). Privacy and Disclosure on Facebook: Youth and Adults' Information Disclosure and Perception of Privacy Risks. Social Psychological and Personality Science, 3(1).

FiveRights Foundation. (2021). Pathways: How Digital Design Puts Children at Risk. Retrieved from https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.

Fogg, B. J. (1999). Persuasive Technologies. Communications of the ACM, 42(5), 26–29.

Fogg, B. J. (2002). Persuasive Technology: Using Computers to Change What We Think and Do. Ubiquity, 2002(2). https://doi.org/10.1145/764008.763957.

Fourie, P. (2020). The political management of pandemics: Global health governance and the securitisation of disease. In *The South African response to COVID-19: The early years*. Routledge.

Fourie, L. (2022). Protecting Children in the Digital Society. In J. Grobbelaar & C. Jones (Eds.), Childhood Vulnerabilities in South Africa. African Sun Media, SUN Press.

Fukuyama, F. (2004). Transhumanism. Foreign Policy, (144), 42–43.
Hauskeller, M. (2012). Utopian Themes in Transhumanist Thought. The Hastings Center Report, 42(2), 39–47.
Heckman E. Carey and Wobbrock O. J. (2000) Put Your Best Face Forward: Anthropomorphic Agents, E-Commerce Consumers, and the Law. Proceedings of the Fourth International Conference on Autonomous agents, p. 435–442.
King, E., & Page, J. (2017). Posthumanism and the Graphic Novel in Latin America. UCL Press.
Kühn, S., Romanowski, A., Schilling, C., et al. (2011). The neural basis of video gaming. Translational Psychiatry, 1, e53. https://doi.org/10.1038/tp.2011.53.
Le Bon, G. (1989). Psihologija gomila. Zagreb: Globus.
Livingstone, S. (2004). What is media literacy? Intermedia, 32(3), 18–20.
Martens, H. (2010). Evaluating media literacy education: Concepts, theories, and future directions. Journal of Media Literacy Education, 2(1).
More, M. (1996). Transhumanism: Towards a Futurist Philosophy. Retrieved from http://www.maxmore.com/transhum.htm.
OFCOM. (2019). Children and parents: Media use and attitudes report 2024—interactive data. Retrieved from https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2024-interactive-data.
Perišić, N. (2021). Šošana Zubof: Doba nadzornog kapitalizma. CM: Communication and Media, 16(50), 337–346.
Potter, W. J. (2022). Analysis of definitions of media literacy. Journal of Media Literacy Education, 14(2), 27–43. https://doi.org/10.23860/JMLE-2022-14-2-3.
Reviglio, U., & Agosti, C. (2020). Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media. Social Media and Society, 1–12.
Rosenbaum, J. E., Beentjes, J. W. J., & Konig, R. P. (2008). Mapping media literacy key concepts and future directions. Annals of the International Communication Association, 32(1).
Ruffo, G., et al. (2023). Studying Fake News Spreading, Polarisation dynamics, and Manipulation by Bots: A tale of Networks and Language. Computer Science Review, 47, 100531.
Sand, M., & Jongsma, K. (2016). Towards an Ageless Society: Assessing a Transhumanist programme. In E. Dominguez-Rue & L. Nierling (Eds.), Ageing and technology. Transcript Verlag.
Slavujević, Z. Đ. (1997). Starovekovna propaganda: Od Vavilonske kule do "Panem et circenses!". Beograd: Radnička štampa.
Vuksanović, D. (2020). Estetsko i stvarno: Mediji–umetnost–život. Zbornik radova FDU br. 37, Fakultet dramskih umetnosti u Beogradu, 113–124. ISSN 1450–5681.
Yeung, K. (2018). Five Fears About Mass Predictive personalisation in an Age of Surveillance Capitalism. International Data Privacy Law, 8, 258–269.
Zuboff, S. (2015). Big Other: Surveillance Capitalism and the prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89.