ROUTLEDGE

Technology, Energy and Warfare in Evolving Geopolitics

Edited by Sandeep Tripathi and Kirill Sablin

Technology, Energy and Warfare in Evolving Geopolitics

This book puts forward a new conceptual framework for emerging geopolitics through the lens of technology, energy, and warfare. Drawing on rich case studies from across the globe, it illuminates how power dynamics are being fundamentally reshaped across nations, governments, international organizations, and individuals.

It highlights three interrelated aspects of the evolving geopolitics: the close connections between technology and geopolitics, and their mutual influence; the interaction between energy and geopolitics, and the problem of ensuring global security; and warfare affecting global politics. The volume discusses cutting-edge trends and developments in artificial intelligence, the expanding domain of cyberwarfare as well as hybrid warfare, ongoing energy transitions, emerging renewable energy hubs, and structural shifts in global energy markets. Through rigorous analysis, the authors track the economic, social, and political transformations triggered by these interconnected developments across the international landscape.

This book will be of great interest to scholars and researchers of international relations, security and intelligence studies, information technology, and artificial intelligence. It will also be of special interest to professionals such as policymakers, security and intelligence practitioners, and professionals working with embassies.

Sandeep Tripathi is the Founding Director of the Forum for Global Studies, New Delhi. He is also a Visiting Professor at the Institute of History and International Relations, Southern Federal University, Russia. He received his PhD in International Relations from Jawaharlal Nehru University, New Delhi. He has delivered keynote addresses at renowned global institutions, including the University of São Paulo, Brazil, Saint Petersburg State University, Russia, Yerevan State University, Armenia, the University of Warsaw, Poland, IDSC, Philippines. He is a regular foreign affairs commentator featured in leading media outlets.

Kirill Sablin is a researcher specializing in political and economic aspects of traditional energy development and discrete structural alternatives of the world economy institutional organization. He received his PhD in Economics from Kemerovo State University, Kemerovo. Currently, he is a Visiting Researcher at the Federal Research Centre of Coal and Coal Chemistry, Kemerovo, Russia. His scientific interests include economic development of countries with emerging markets, Schumpeterian innovations, rent-seeking behavior, political connections in resource-abundant economies, and technological sovereignty of extractive industries. His expertise spans over the construction of models of complex economic processes using the theory of fuzzy sets.

Technology, Energy and Warfare in Evolving Geopolitics

Edited by Sandeep Tripathi and Kirill Sablin

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Designed cover image: Getty Images

First published 2026
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-041-04920-3 (hbk)
ISBN: 978-1-041-05969-1 (pbk)
ISBN: 978-1-003-63320-4 (ebk)

DOI: 10.4324/9781003633204

Typeset in Times New Roman
by SPi Technologies India Pvt Ltd (Straive)

Contents

Contributors

Chakali Bramhayya, Associate Professor, Department of Political Science, Faculty of Arts, University of Allahabad, Prayagraj, India.

Bharti Das, Professor and Head, Department of Defence and Strategic Studies, University of Allahabad, Prayagraj, India.

Soumyodeep Deb, PhD Fellow, Government and International Affairs, Lingnan University, Hong Kong.

Gusti Aju Dewi, AI-Behavior Intelligence Strategist, Indonesian Pioneer & Global Expert Graphologist, Masters Candidate in Computer Science (AI Specialist), Indonesia.

Mohd Faheem, Assistant Professor of Indian Studies at Pridi Banomyong International College, Thammasat University, Bangkok, Thailand.

Saddam Hussain, Assistant Professor of Political Science at Government General Degree College, Dantan-II, West Medinipur, West Bengal, India.

Himani Kaushik, Assistant Professor Grade 2, School of Law, UPES, Dehradun, India.

Achal Malhotra, Former Ambassador of India to Armenia and Georgia, Former Deputy Permanent Representative of India to UN and International Organizations in Vienna, currently he is a Managing Editor at Indian Foreign Affairs Journal, New Delhi, India.

Amna Mirza, Associate Professor, Department of Political Science, SPM College, University of Delhi, India.

Zeeshan Munir, Academic Associate at IIM Kashipur, Uttarakhand, India.

Bishnu Pandey, Mechanical Engineer and Researcher, Green Hydrogen Lab, Department of Mechanical Engineering, Kathmandu University, Nepal.

Shalendra D. Sharma, Associate Vice President and Lee Sahu Kee Foundation Chair Professor of Political Science, Lingnan University, Hong Kong.

Manjari Singh, Associate Editor, Journal of World Affairs: Voice of the Global South (Sage) and author of "India and the Gulf: A Security Perspective" (London: Routledge), India.

Uday Pratap Singh, Assistant Professor, ISDC, University of Allahabad, Prayagraj, India.

Sanjay Soi, (Retd). Major General of Indian Army and Advisor to Forum for Global Studies, New Delhi, India.

Patrick C. R. Terry, Dean of the Faculty of Law and a Professor of Law at the University of Public Administration in Kehl, Germany.

Biraj Singh Thapa, Associate Professor in Mechanical Engineering at Kathmandu University, Dhulikhel, Nepal.

Devesh Vatsa, Advisor to Data Security Council of India, New Delhi, India.

Tewodros Woldearegay, PhD Fellow, Lingnan University, Hong Kong.

Idris Yeba Buta, Assistant Professor of International Relations at Jimma University, Ethiopia.

1 Introduction

Sandeep Tripathi and Kirill Sablin

The modern world is characterized by a complex interweaving of processes and phenomena that are transforming the nature of relations between countries, governments, international organizations and individuals. In recent years, events have shown that changes in the international panorama are determined mostly with geopolitical trends that are developing in different parts of the world. At the same time, the geopolitical sphere itself is strongly influenced by certain factors that lead to challenges and shocks, both internal and external ones. In this sense various alternatives of further development of the world order are emerged. To offer just one example, J.S. Nye Jr. noted that the prospect of a wholly disengaged, self-focused United States has troubling implications for the world order.[1] This will affect every other country, because of the interconnected relationships among states and other major transnational actors. A world order rests on a stable distribution of power among states, norms that influence and legitimize conduct and shared institutions. Relations among states naturally vary over time, thus in this case the status of the world order is the matter of its perception by the contemporaries. Its evolution is fueled by the crucial factors that determine the main frame of geopolitics.

The first factor that shapes the new outlines of transforming geopolitics is technology. We understand this factor in the broad sense, i.e. as a driver and game changer that brings advantages to those beneficiaries who harvested the positive effects of current and very sharp industrial transformation called the Fourth Industrial Revolution. This revolution is describing the rapid and irreversible technological advances in the 21st century. As a part of the overall industrial changes, Fourth Industrial Revolution involves the joining up of technologies such as artificial intelligence (AI), gene editing, and advanced robotics that blur the lines between the physical, digital, and biological worlds. Fundamental shifts are taking place in how the global production and supply chains operate through the automation of traditional manufacturing and industrial practices, using modern technologies, large-scale machine-to-machine communication, and the Internet of Things. Like the revolutions that preceded it, it is more than likely that the Fourth Industrial Revolution has the potential to raise global income levels and improve the quality of life for populations around the world. Technological innovation will also lead to rapid

DOI: 10.4324/9781003633204-1

supply-side growth, with long-term gains in efficiency and productivity. Transportation and communication costs will drop, logistics and global supply chains will become more effective, and the cost of trade will diminish. However, the development of technologies involves not only a positive side that is manifested in economic growth, various innovations, and reductions in costs. Indeed, technological development leads to profound changes and the deepening digitalization of economies and societies. At the same time, technology has become a battleground in the geopolitical quest for power. New technologies such as AI, nanotechnology, and robotics have become more intertwined with the geopolitical, economic, and trade interests of the nations. Technological rivalries are broadly divided between countries promoting liberal governance models and those deploying technology to support authoritarian regimes. Technology is also at the core of geopolitical struggles through its deployment in cyberwarfare, election interference, and misinformation. A case in point is that of Israel, where technology has been a cornerstone of the country's survival and its economic growth. In the face of geographical challenges, especially those marked by arid land and limited natural resources, Israel harnessed technological innovation to transform its agriculture and has proven successful in turning its desert land into fertile ground. More importantly, technology remains central to the country's national strategy, driving its economic growth, security, and global influence. Another case is the semiconductor sector, which is a battlefield between the USA and China. Semiconductors are the brains of modern electronics, empowering technologies critical to countries' economic growth, national security, and global competitiveness. They secure advances in communications, computing, military systems, clean energy, and countless other applications. Currently, Taiwan's dominance in the global semiconductor supply chain has made it a critical player in the modern economy. The escalating tensions between China and Taiwan, fueled by China's assertive push for reunification and Taiwan's resistance to these moves, have exposed the limitations of economic interdependence in preventing conflict. Despite China's reliance on the Taiwanese semiconductor industry, it has not hesitated to engage in military drills and activities around the Taiwan Strait.

The second factor that shapes the new outlines of transforming geopolitics is energy. The intersection of geopolitics and energy is a critical area of interaction between state and non-state actors. Moreover, new challenges are raised linked with sustainable development issues and a transition to renewable energy resources. A much closer issue is the intersection of geopolitics and energy security. The combination of energy and geopolitics can disrupt regional stability and has major effects on global energy markets. The evolving global energy system calls for a proactive strategy to shape interdependencies and bolster the resilience of the energy system, enabling it to adapt not only to changes within the energy sector but also to wider economic, social, and political shifts. Southeast Asia is one of the important regions in the context of climate change and the need to alter the energy sector to promote clean and green technology. This is one of the rapidly developing and strategically located

regions and it faces the dual challenges of pursuing sustainable development and intensifying great-power competition, particularly between the United States and China. Another case is that of the development of Nepal as a hydrogen hub for a contribution to energy transition and green growth in South Asia. The rising geopolitical pressure induced by climate change is forcing an increase in the share of renewable energy. The production of green hydrogen from renewable energy sources and its application in the hard-to-abate sectors are becoming prominent solutions for Nepal's economy. Another region to demonstrate the obvious link between energy and geopolitics is the Horn of Africa (HoA). Due to its strategic location at the southwest gate to the Red Sea, thereby linking European markets with Africa, the Middle East, and Asia, this region has historically been a hotspot for great-power competition. Relationships between energy security, geopolitics, and foreign interventions in the HoA impact regional stability and shape the future contours of social and economic development.

The third factor to shape the new outlines of transforming geopolitics is warfare. One may state that geopolitics and warfare are complementary terms and unified processes. The permanent importance of territory with the resources, as well as the current trends in the development of battlefield methods, actualize the link between geopolitics and warfare. One of the examples is the use of AI, which emerges as a game changer in defining the nature of warfare. This technology reshapes cyber security strategies; it plays a vital role in cognitive warfare and also amplifies traditional propaganda. Using the case of India, the book highlights the changing dimensions of warfare, including its increasingly hybrid nature.

Note

1 Nye, J.S. Jr., The Future of World Order/Project Syndicate, https://www.project-syndicate.org/commentary/future-of-world-order-second-trump-presidency-american-decline-by-joseph-s-nye-2025-03.

Part I

Technology and Geopolitics

2 Fourth Industrial Revolution and Global Governance

Understanding Reshaping of Contours of Human Security

Amna Mirza

Introduction

The Fourth Industrial Revolution (4IR) is an epochal transformation that is reshaping human civilization's very essence. Its profound impact reverberates through the spheres of technology, economics, society, and politics, transcending borders and boundaries. In tandem with this seismic shift, the landscape of global governance is undergoing a profound metamorphosis, as the established norms and frameworks that have governed international relations for decades are being redefined. To understand the significance of 4IR in the context of global governance, we must first delve into the historical underpinnings of international relations. Traditionally, theories such as political realism and neo-realism have provided the bedrock for our comprehension of global affairs. These perspectives, rooted in post-World War II geopolitical realities, have emphasized the primacy of the nation-state as the central actor in international relations. Concepts like self-help, statism, and the relentless pursuit of national survival have been the main anchors of this worldview.

However, the post-Cold War era marked a watershed moment in the evolution of international relations theory. It compelled us to revisit and revise our understanding of security and national interest. No longer could we confine our analysis to the traditional dimensions of security, such as military might and territorial integrity. Instead, a more holistic, multidimensional perspective emerged, acknowledging that security encompassed a broad spectrum of facets, including economic stability, food security, access to healthcare, environmental sustainability, personal safety, community cohesion, and political stability. This re-evaluation of security culminated in the United Nations Development Programme's, 1994 World Development Report, which introduced the concept of "human security." This paradigm shift emphasized the importance of individual agency and well-being, transcending the confines of the nation-state. It recognized that genuine security could only be achieved by addressing the myriad concerns that affect individuals on a daily basis, from economic hardships to environmental threats and political instability.

The historical trajectory of industrial revolutions has played a pivotal role in shaping global governance issues. The First Industrial Revolution,

DOI: 10.4324/9781003633204-3

characterized by the mechanization of production processes, powered the imperialistic ambitions of the 19th century, laying the groundwork for colonialism and ultimately contributing to the cataclysmic First World War. Subsequent phases of the Industrial Revolution, the Second and the Third, were instrumental in propelling globalization. The Second Industrial Revolution saw the rise of mass production and the assembly line, fundamentally altering the dynamics of trade and commerce. The Third Industrial Revolution, marked by the advent of computers and digital technology, brought about a connected world, where information flowed seamlessly across borders.

Now, we find ourselves on the precipice of the Fourth Industrial Revolution, an era distinguished by rapid technological advancements, the proliferation of artificial intelligence, the Internet of things (IoT), and the digitalization of almost every facet of human existence. The Fourth Industrial Revolution has ushered in an era of unprecedented connectivity and transformation, demanding an innovative approach to understanding its implications for human security. In this chapter, we will explore the intricate relationship between the Fourth Industrial Revolution and the terrain of global governance. It will elucidate how this revolution is redefining our imaginations concerning the components that constitute human security in an era marked by both unparalleled opportunities and daunting challenges. The following sections will delve into the impact of 4IR on global governance, discuss the emerging risks and ethical considerations, and propose strategies to navigate this new reality effectively. As we embark on this exploration, it is abundantly clear that the Fourth Industrial Revolution is not merely a technological revolution; it is a transformative force reshaping the contours of human security and global governance.

Review of Literature

The literature reviewed in this section presents a rich tapestry of ideas, perspectives, and analyses. These works collectively underscore the complexity and interconnectedness of the Fourth Industrial Revolution, global governance, human security, and globalization. They illuminate the multifaceted nature of 4IR, emphasizing its transformative potential as well as the ethical, socioeconomic, and geopolitical challenges it poses.

1 Klaus Schwab's Vision of the Fourth Industrial Revolution

Schwab's seminal work, *The Fourth Industrial Revolution* (Schwab, 2017), serves as an indispensable cornerstone for comprehending the technological underpinnings of 4IR and its ramifications. As the founder of the World Economic Forum (WEF), Schwab elucidates the pivotal role of emerging technologies—AI, the IoT, biotechnology, and more—in driving a new industrial revolution. Beyond its technological dimension, Schwab's work introduces us to the transformative potential of 4IR in various domains, from healthcare to governance, laying a foundation for our understanding.

His emphasis on the "Fourth Industrial Revolution" extends beyond technology to its socioeconomic and geopolitical ramifications. He underscores that the changes driven by 4IR are not merely incremental but are, in fact, systemic in nature, affecting every aspect of our lives. From reshaping industries to influencing the nature of work and the structure of economies, Schwab's work underscores that the Fourth Industrial Revolution is not a future possibility; it is a present reality that necessitates immediate attention from policymakers, scholars, and society as a whole.

2 The Evolving Landscape of Global Governance

As we shift our focus to global governance, the work *The Globalization of World Politics: An Introduction to International Relations* (2018), edited by John Baylis, Steve Smith, and Patricia Owens, offers an invaluable resource. This comprehensive volume elucidates the multifaceted realm of international relations, exploring the role of global institutions, nation-states, and non-state actors in navigating the challenges of globalization and technological progress. The book provides a broad backdrop for understanding the evolving global governance landscape in the context of 4IR. Baylis, Smith and Owens' work delves into the dynamics of global governance, emphasizing the complexities that emerge as technology and globalization continue to advance. It highlights the shifting power structures and the evolving nature of diplomacy in an interconnected world. Furthermore, it draws attention to the challenges posed by global issues such as climate change, cybersecurity, and economic inequality, which transcend national boundaries and require collaborative efforts in the era of 4IR.

3 Human Security in the Age of the Fourth Industrial Revolution

Human security in the Fourth Industrial Revolution emerges as a relevant and insightful aspect. It delves into the multidimensional aspects of human security and aligns them with the challenges and opportunities presented by 4IR. It underscores the need to shift the focus from traditional state-centric security to safeguarding individuals in an interconnected world. It is emphasized the complex and evolving nature of human security in the age of 4IR. The aspect contend that the concept of security must expand beyond military and political dimensions to address issues such as economic stability, access to healthcare, environmental sustainability, and personal safety. Through a series of case studies and analyses, it illustrates how the Fourth Industrial Revolution is transforming the dynamics of human security and, consequently, necessitating innovative approaches to its preservation.

4 Globalization, Technology, and Human Development

While not explicitly centered on 4IR, Amartya Sen's *Development as Freedom* (1999) provides a foundational perspective on the interplay between globalization, technology, and human development. Sen's capabilities approach argues that human freedom and well-being should be central to development processes. In the context of 4IR, this perspective gains renewed relevance as it underscores the importance of harnessing technological

advancements for the betterment of human lives. Sen's work highlights the ethical imperative of ensuring that the benefits of globalization and technological progress are distributed equitably. He argues that development should be assessed not merely in terms of income but also in terms of people's capabilities and opportunities. Sen's insights prompt us to consider how the revolution can be harnessed to enhance human development, reduce inequality, and promote individual freedoms.

5 The Dark Side of 4IR: Emerging Risks and Ethical Dilemmas

Ethical considerations and emerging risks associated with 4IR come to the forefront in *The Age of Surveillance Capitalism* by Shoshana Zuboff (2019). Zuboff's work delves into the rise of surveillance capitalism, a phenomenon where personal data is harvested for profit, often without individuals' informed consent. This surveillance capitalism poses profound ethical dilemmas and threatens individual autonomy and human rights. Zuboff's meticulously researched book serves as a cautionary tale, highlighting the need for ethical frameworks and regulations to guide the development and deployment of advanced technologies in the era of 4IR. She underscores the urgency of addressing issues related to data privacy, surveillance, and the manipulation of human behavior in an age where technology companies wield unprecedented power.

6 Globalization and Inequality: Joseph Stiglitz's Perspective

Joseph Stiglitz's *Globalization and Its Discontents Revisited: Anti-Globalization in the Era of Trump* (2017) provides a critical examination of globalization and its effects on inequality. While not focused on 4IR, it offers a nuanced perspective on the potential socioeconomic consequences of technological advancements and globalization in the context of 4IR. Stiglitz argues that the benefits of globalization have not been evenly distributed, leading to increased disparities in wealth and opportunities. His analysis prompts us to consider how 4IR may exacerbate or mitigate these inequalities, especially as it reshapes industries and the nature of work. Stiglitz's insights underscore the imperative of addressing socioeconomic disparities in the age of 4IR and devising inclusive policies that ensure equitable access to its benefits.

7 The Role of International Organizations in 4IR Governance

In the realm of international governance mechanisms for the Fourth Industrial Revolution, *Global Governance and the Emergence of Global Institutions for the 21st Century*, edited by Augusto Lopez-Claros, Arthur L. Dahl and Maja Groff (2020), offers valuable insights. This edited volume delves into the role of international organizations, such as the World Trade Organization and the World Health Organization, in addressing the challenges posed by 4IR. It sheds light on the evolving landscape of global governance in response to technological disruptions. Lopez-Claros and Dahl's work emphasizes the importance of international cooperation and the need for institutions that can effectively navigate the complexities of 4IR. They discuss how international organizations are adapting to the digital age,

addressing issues such as trade in the digital economy, cybersecurity, and global health in the context of emerging technologies. The book highlights the role of multilateralism in shaping the governance of 4IR and underscores the necessity of collaborative efforts on a global scale.

8 The Fourth Industrial Revolution and Geopolitical Shifts

Kishore Mahbubani's *Has the West Lost It? A Provocation* (2018) offers a provocative perspective on how the Fourth Industrial Revolution is influencing geopolitical dynamics. Mahbubani argues that the West's dominance is waning in the face of rapid technological progress in Asia and other regions. His insights prompt us to consider how 4IR is reshaping not only global governance but also the geopolitical balance of power. Mahbubani's work underscores that the geopolitical implications of 4IR extend beyond economics and technology to questions of global influence and leadership. He challenges conventional wisdom about the West's pre-eminence and calls for a re-evaluation of existing geopolitical narratives. In the context of 4IR, Mahbubani's perspective invites us to examine how emerging powers are leveraging technological advancements to redefine the geopolitical landscape.

Central Question

This chapter is guided by two central questions that serve as the fulcrum of our exploration. First, we inquire into the multifaceted impact of the Fourth Industrial Revolution on various dimensions of human security. In this age of unprecedented technological advancements, how have economic, environmental, health, personal, and political aspects of human security been reshaped? Second, we delve into the intricate interplay between the Fourth Industrial Revolution, human security, and global governance. How are the complex and interconnected aspects of human security influenced by the ongoing transformation brought about by the Fourth Industrial Revolution? These central questions frame our analysis and guide us in unravelling the profound implications of 4IR on the well-being and stability of individuals, communities, and the global order.

Understanding Human Security

In an increasingly complex and interconnected world, human security has emerged as a powerful and comprehensive approach to address the myriad challenges that individuals and communities face. This approach recognizes that the contemporary global landscape is marked by a multitude of threats and insecurities, ranging from protracted crises and violent conflicts to natural disasters, persistent poverty, epidemics, and economic downturns. These challenges, often overlapping and intertwined, can have far-reaching consequences, eroding the foundations of peace, stability, and sustainable development. It stands as a powerful analytical and planning framework, enabling more encompassing and preventive responses by the United Nations and its

partners. It transcends traditional sectoral boundaries, fosters contextually relevant solutions, and champions partnerships in the pursuit of a world free from fear, want, and indignity. As articulated in General Assembly resolution 66/290, human security offers a framework to assist member states in identifying and confronting these widespread and cross-cutting challenges that affect the survival, livelihood, and dignity of their people. It calls for responses that are people-centered, comprehensive, context-specific, and prevention-oriented, with a primary focus on enhancing the protection and empowerment of all individuals.

Promoting Multi-Stakeholder Partnerships

Central to the human security approach is the mobilization of expertise and resources from a diverse array of actors. These actors include the United Nations system, governments, the private sector, civil society, and local communities. By bringing together this wide range of stakeholders, human security leverages synergies, capitalizing on the unique strengths and advantages that each actor brings to the table.

Localization and 'Leaving No One Behind'

Human security recognizes the heterogeneity of challenges across countries and communities. It acknowledges that the root causes and manifestations of insecurity vary significantly from one context to another. Therefore, it promotes responses that are grounded in local realities, emphasizing the need to localize international and national agendas. The overarching goal is to ensure that no one is left behind in the pursuit of security and well-being.

Prevention and Resilience

At its core, human security is driven by a commitment to prevention. It seeks to address the underlying vulnerabilities that give rise to insecurity, focusing on early action to mitigate emerging risks. This approach strengthens local capacities to build resilience and champions solutions that foster social cohesion while upholding the principles of human rights and dignity. In sum, human security offers a comprehensive and holistic perspective on security challenges in the contemporary world. It recognizes that security is not solely about safeguarding territorial integrity or military defense; rather, it encompasses a wide spectrum of interconnected dimensions that impact the lives of individuals and communities. As we navigate the Fourth Industrial Revolution and the transformations it brings, understanding the multifaceted nature of human security becomes increasingly essential. The 4IR introduces new dimensions of both opportunity and risk, and the human security approach provides a robust foundation for comprehending and addressing these complex challenges while upholding the well-being and dignity of all individuals and communities.

The UNDP 1994 World Development Report: A Paradigm Shift in Security

The UNDP's 1994 World Development Report, subtitled *New Dimensions of Human Security*, marked a significant departure from traditional approaches to security. Prior to this report, security was predominantly framed within the context of state-centric national security, focusing on military capabilities and territorial integrity. The end of the Cold War and the evolving global landscape necessitated a reevaluation of these conventional security paradigms.

The UNDP's report introduced a paradigm shift by emphasizing the centrality of human beings in security considerations. It challenged the notion that security could be divorced from the well-being of individuals and communities. This novel approach expanded the scope of security to encompass seven interrelated dimensions:

1 **Economic Security**: Recognizing the importance of stable access to resources, employment, and economic opportunities for individuals and communities.
2 **Food Security**: Highlighting the need for consistent access to sufficient, safe, and nutritious food to lead a healthy life.
3 **Health Security**: Addressing the availability of healthcare, disease prevention, and protection against health-related risks.
4 **Environmental Security**: Acknowledging the necessity of a sustainable environment and the mitigation of environmental threats to human well-being.
5 **Personal Security**: Emphasizing protection against violence, crime, and human rights abuses, including physical and psychological safety.
6 **Community Security**: Focusing on social cohesion, stable community relationships, and resilience against social disruptions.
7 **Political Security**: Encompassing the protection of basic human rights, political freedoms, and participation in decision-making processes.

The 1994 report articulated that these seven dimensions were inseparable and interconnected. Neglecting any one of them could undermine overall human security. This holistic approach recognized that security was not merely the absence of conflict but the presence of conditions that allowed individuals to live in dignity and freedom.

Human Security in the Fourth Industrial Revolution

Fast-forward to the Fourth Industrial Revolution, where technological innovations and digital transformations are rapidly reshaping our world. The impact of 4IR on the dimensions of human security cannot be overstated. The digital economy and automation have disrupted traditional employment patterns, leading to concerns about job displacement and economic inequality. However, 4IR also presents opportunities for economic growth, entrepreneurship, and

innovation. Achieving economic security at the age of 4IR requires policies that promote equitable access to economic opportunities and support reskilling and upskilling to adapt to the changing job landscape. Technological advancements in agriculture, such as precision farming and biotechnology, have the potential to revolutionize food production and distribution. However, these innovations also raise questions about the environmental impact of modern agriculture and equitable access to food resources. Ensuring food security in the context of 4IR entails sustainable agricultural practices and equitable food distribution systems.

Health Security in 4IR: 4IR has transformed healthcare through telemedicine, wearable health devices, and the use of big data for disease monitoring. While these innovations improve healthcare accessibility and outcomes, they also pose challenges related to data privacy and cybersecurity. Balancing the benefits and risks of 4IR in healthcare is crucial for maintaining health security. The Fourth Industrial Revolution has brought both opportunities and threats to environmental security. While clean technologies and data-driven approaches can contribute to environmental sustainability, the rapid pace of technological change can also exacerbate environmental degradation. Environmental security in 4IR necessitates a commitment to green technologies, responsible resource management, and global cooperation on climate action.

The digital age has given rise to new forms of personal security threats, including cyberattacks, online harassment, and breaches of privacy. At the same time, technology can enhance personal security through surveillance systems, emergency response apps, and advanced authentication methods. Striking a balance between personal security and individual privacy is a paramount concern in the Fourth Industrial Revolution. Communities are both beneficiaries and victims of 4IR. While digital connectivity and social media enable community building and information sharing, they also expose communities to risks such as misinformation, online radicalization, and social disruption. Safeguarding community security in 4IR involves promoting digital literacy, countering online extremism, and fostering inclusive online spaces.

The digital realm has become a new battleground for political security, with concerns about cyberattacks on critical infrastructure and interference in democratic processes. Protecting political security in the Fourth Industrial Revolution requires robust cybersecurity measures, international norms, and digital governance frameworks that ensure the integrity of political systems. In sum, the UNDP's 1994 World Development Report laid the groundwork for redefining security as human security, encompassing a holistic view of well-being and emphasizing the interconnectedness of various dimensions of security. In the context of the Fourth Industrial Revolution, this paradigm remains relevant, guiding us in understanding the multifaceted impact of 4IR on human security. The interplay between 4IR and these dimensions of human security is complex and evolving, and addressing the challenges and opportunities it presents requires a nuanced and adaptable approach.

Towards the Fourth Industrial Revolution: Understanding the Phases of Transformation

The Fourth Industrial Revolution is not just a buzzword; it represents a seismic shift in the way we live, work, and interact with the world around us. To comprehend the full impact of 4IR on human security and global governance, it is imperative to delve into its evolution through four distinct phases. Each phase builds upon the innovations of its predecessor, creating a continuum of technological progress that has reshaped the contours of human civilization.

The journey towards 4IR commences with the First Industrial Revolution, an era characterized by the mechanization of labor-intensive tasks. This period, spanning the late 18th century to the mid-19th century, witnessed the advent of steam engines, mechanized textile production, and the mechanization of agriculture. It marked a profound shift from agrarian economies to industrial ones, leading to urbanization and a reconfiguration of societal structures. Key innovations included the steam engine, the spinning jenny, and the power loom. These technological advancements revolutionized manufacturing processes, significantly increasing productivity and changing the nature of work. However, they also brought about social and economic upheaval, as traditional cottage industries were replaced by large-scale factories, leading to labor displacement and societal unrest.

The Second Industrial Revolution, occurring from the late 19th century to the early 20th century, was marked by the widespread adoption of electricity and the emergence of mass production techniques. Innovations like the telegraph, telephone, and the assembly line transformed communication, transportation, and manufacturing. Thomas Edison's invention of the practical incandescent light bulb and the development of alternating current (AC) electrical systems by Nikola Tesla and George Westinghouse were pivotal advancements during this period. These innovations not only revolutionized daily life but also laid the foundation for the electrification of industries and homes. The assembly line, introduced by Henry Ford, further streamlined production processes and enabled the mass production of automobiles. The Second Industrial Revolution ushered in an era of increased urbanization, the rise of consumer culture, and a growing dependence on electricity and fossil fuels.

The Third Industrial Revolution, often referred to as the Digital Age, unfolded from the late 20th century to the early 21st century. It was characterized by the rapid proliferation of digital technologies, the rise of the internet, and the advent of personal computing. Key innovations included microprocessors, the World Wide Web, and mobile communication technologies. The microprocessor, invented by Intel in 1971, miniaturized computing power and paved the way for personal computers and the automation of various tasks. Tim Berners-Lee's creation of the World Wide Web in 1989 revolutionized information access and communication, connecting people across the globe. The Third Industrial Revolution ushered in an era of unparalleled connectivity, data

sharing, and technological convergence. It led to the development of e-commerce, social media platforms, and the digitalization of industries such as finance, healthcare, and entertainment. The impact of the digital age on human society and global governance cannot be overstated, as it reshaped communication, information dissemination, and economic structures.

The Fourth Industrial Revolution, the current phase, represents a convergence of digital, biological, and physical innovations. It is characterized by the integration of cyber-physical systems, artificial intelligence, biotechnology, and the Internet of Things (IoT). This phase, which began in the early 21st century, has ushered in a new era of transformation with profound implications for human security and global governance. AI and machine learning have enabled machines to process and analyze vast amounts of data, leading to advancements in autonomous vehicles, healthcare diagnostics, and predictive analytics. The IoT has interconnected everyday objects, creating smart homes, cities, and industries. Biotechnology breakthroughs, such as gene editing and personalized medicine, are revolutionizing healthcare and agriculture.

The Fourth Industrial Revolution is marked by the blurring of physical and digital boundaries, as exemplified by autonomous robots and smart manufacturing systems. It has the potential to revolutionize industries, enhance productivity, and address global challenges such as climate change and healthcare access. However, it also raises ethical and societal concerns, including job displacement, data privacy, and the potential misuse of AI. In essence, the journey towards the Fourth Industrial Revolution has been shaped by these four distinct phases, each building upon the innovations of its predecessor. As we navigate the complex landscape of 4IR, understanding its evolutionary path is essential to comprehending the multifaceted impact it has on human security and global governance. In the following sections, we will explore how 4IR is reshaping the dimensions of human security and redefining the contours of global governance in an era characterized by technological convergence and unprecedented connectivity.

Globalization 4.0: Navigating the New Global Landscape

Globalization, a concept that has evolved through multiple iterations, now stands at the cusp of its fourth phase, aptly labeled "Globalization 4.0." This latest phase of globalization is defined by the convergence of technological, economic, social, and environmental forces that are reshaping the world in unprecedented ways. Understanding Globalization 4.0 is crucial, as it plays a pivotal role in the ongoing transformation of human security and global governance. To appreciate the significance of Globalization 4.0, we must first take a step back and trace the evolution of globalization. It began with the First Industrial Revolution in the late 18th century, which saw the mechanization of labor-intensive tasks and the emergence of steam-powered machinery. This era marked the advent of global trade, as goods could be produced on a scale never before seen and transported across oceans.

The Second Industrial Revolution, characterized by the widespread adoption of electricity and mass production techniques in the late 19th and early 20th centuries, further accelerated globalization. Innovations such as the telegraph, telephone, and assembly line transformed communication and manufacturing, facilitating global supply chains and intercontinental trade. The Third Industrial Revolution, also known as the Digital Age, began in the late 20th century with the proliferation of digital technologies, the rise of the internet, and the advent of personal computing. This phase saw the globalization of information and the emergence of a globally interconnected economy driven by technology and data.

Key Drivers

Globalization 4.0 represents a new era of hyperconnectivity, where the boundaries between the physical, digital, and biological worlds are blurred. This phase is characterized by several key drivers:

1 Technological Advancements: Technologies like artificial intelligence, the Internet of Things (IoT), blockchain, and 5G are reshaping industries and enabling real-time global communication and data exchange. These technologies are revolutionizing how businesses operate and how societies function.
2 The Fourth Industrial Revolution: As discussed earlier, the Fourth Industrial Revolution (4IR) is a critical component of Globalization 4.0. It is characterized by the integration of cyber-physical systems, AI, biotechnology, and more. These innovations are transforming industries, economies, and societies on a global scale.
3 The Rise of Digital Platforms: Digital platforms and ecosystems are fostering connectivity and collaboration on an unprecedented scale. Companies like Amazon, Alibaba, and Google have created global platforms that transcend borders, offering services and products to a global customer base.
4 Environmental Considerations: Globalization 4.0 is increasingly focused on environmental sustainability. As climate change and resource depletion become global challenges, international cooperation and sustainability initiatives are central to this phase of globalization.

Impact on Human Security

The implications of Globalization 4.0 for human security are profound and multifaceted. On one hand, technological advancements have the potential to improve living standards, healthcare, education, and access to information. However, they also introduce new challenges, including cybersecurity threats, job displacement due to automation, and privacy concerns related to the collection and use of personal data. The interconnectedness of the global economy means that economic crises and disruptions in one part of the world can

have ripple effects that impact livelihoods and well-being globally. This underscores the importance of addressing economic disparities and ensuring equitable access to the benefits of globalization.

Impact on Global Governance

Globalization 4.0 presents both opportunities and challenges for global governance. While it enables enhanced international cooperation and the sharing of knowledge and resources, it also raises questions about the adequacy of existing governance structures. Issues like data privacy, intellectual property rights, and the regulation of emerging technologies require innovative approaches and international collaboration. In this new era, global governance must be agile, inclusive, and responsive to the rapidly changing dynamics of the global landscape. Multilateral organizations, governments, and civil society must work together to address transnational issues, promote sustainable development, and uphold the principles of human rights in an interconnected world.

Embracing Globalization 4.0

Globalization 4.0 represents a transformative phase in the evolution of globalization, driven by technological advancements, environmental imperatives, and new modes of global connectivity. As we navigate this era of hyperconnectivity, it is essential to harness the opportunities it presents while addressing its challenges. To achieve this balance, it is imperative for governments, organizations, and individuals to adapt, innovate, and collaborate on a global scale. By doing so, we can harness the potential of Globalization 4.0 to advance human security, promote sustainable development, and shape a more inclusive and equitable global governance framework for the benefit of all.

The Undefined, Yet Definite Terrain of Global Governance: Navigating Complexity and James Rosenau's Thesis

Global governance, a concept that has gained prominence in recent decades, represents an evolving and multifaceted landscape where states, international organizations, non-state actors, and transnational networks intersect and interact to address complex global challenges. As we explore this dynamic terrain, we delve into the insights of scholars like James Rosenau and the influential ideas of institutions like the World Bank. Together, they offer valuable perspectives on the ever-changing nature of global governance.

James Rosenau, a renowned scholar in the field of international relations, has made significant contributions to our understanding of global governance and the evolving nature of sovereignty. One of his seminal ideas revolves around the concept of "fragmentation" and the "post-international" system. Rosenau's concept of fragmentation encapsulates the idea that globalization is not a linear, uniform process but rather a complex and fragmented one.

He argues that in the post-Cold War era, global governance has become increasingly fragmented, with multiple actors and institutions participating in decision-making processes. This fragmentation is often driven by issue-specific interests and the need for flexible governance arrangements. For example, in addressing climate change, a multitude of actors, including states, non-governmental organizations, and corporations, collaborate in a fragmented, yet coordinated manner to achieve common goals.

The Post-International System: Rosenau challenges the traditional notion of international relations characterized by state-centric diplomacy. He posits that we have entered a "post-international" era, where traditional notions of sovereignty and state authority are being redefined. In this era, global governance extends beyond the realm of intergovernmental relations to encompass a multitude of actors, including non-state entities and transnational networks. The state remains a central actor, but it is no longer the sole determinant of global affairs. Rosenau's insights highlight the evolving nature of global governance, where actors and institutions adapt to the complexities of an interconnected world. The traditional Westphalian system, which emphasizes state sovereignty and non-interference in domestic affairs, is being reconfigured to accommodate the demands of an increasingly interdependent global society.

World Bank Ideas: Shaping the Global Governance Landscape

The World Bank, a prominent international financial institution, has played a significant role in shaping the landscape of global governance, particularly in the realm of economic development and poverty reduction. Its ideas and policies have had far-reaching implications for global governance practices. The World Bank has been a proponent of economic globalization, advocating for market-oriented policies, trade liberalization, and privatization as pathways to economic development. These ideas have influenced the economic governance strategies of many countries, particularly in the Global South. The World Bank's role as a knowledge bank, disseminating economic and development expertise, has contributed to the convergence of economic policies worldwide.

Development Goals: The World Bank has been instrumental in shaping the global development agenda through initiatives like the Millennium Development Goals (MDGs) and, later, the Sustainable Development Goals (SDGs). These frameworks have provided a shared vision for global development efforts, promoting cooperation among states, international organizations, and civil society. The SDGs, in particular, underscore the interconnectedness of global challenges and the need for collaborative governance approaches. While the World Bank's ideas and policies have made significant contributions to global governance, they have also faced criticism. Critics argue that market-oriented reforms have sometimes exacerbated inequalities and social disparities. Additionally, the institution has been accused of imposing 'one-size-fits-all' solutions without considering the diverse contexts and needs of individual countries.

Navigating the Dynamic Terrain

The terrain of global governance is both undefined and definite—an ever-evolving landscape where established concepts like sovereignty are being redefined, and new actors and networks are emerging. James Rosenau's insights on fragmentation and the post-international system remind us that the governance of global affairs is becoming increasingly complex and interconnected. The World Bank's ideas and policies have played a central role in shaping economic governance and development strategies worldwide, influencing the course of global governance. However, these ideas are not without their challenges and critiques, highlighting the ongoing need for adaptive and inclusive approaches to global governance.

As we navigate this dynamic terrain, it is essential to recognize that global governance is no longer the exclusive domain of states but a multifaceted and collaborative endeavor. It requires a nuanced understanding of the evolving roles of various actors, the interplay of interests and values, and the imperative of addressing global challenges collectively. By embracing this complexity and building inclusive governance frameworks, we can better navigate the undefined yet definite terrain of global governance in an interconnected world.

Dimensions of Human Security, Fourth Industrial Revolution & Global Governance: A Multifaceted Discussion

The Fourth Industrial Revolution is reshaping the world in profound ways, with implications that reverberate across the dimensions of human security and the landscape of global governance. In this multifaceted discussion, we explore how 4IR intersects with economic, food, health, environmental, personal, community, and political security, shedding light on the evolving challenges and opportunities in our interconnected world. Economic security, a critical dimension of human security, encompasses access to stable resources, employment opportunities, and financial stability. The advent of 4IR has brought about both promises and perils in this realm. On one hand, automation and AI-driven technologies have the potential to boost productivity and create new industries. On the other hand, there are concerns about job displacement and income inequality as automation replaces certain tasks and industries. Global governance mechanisms must adapt to ensure equitable access to the benefits of technological advancements and address the economic disparities that may arise. Food security, the assurance of consistent access to safe and nutritious food, is essential for human well-being. 4IR technologies are being harnessed to enhance food production and distribution, from precision agriculture to blockchain-based supply chain management. However, environmental challenges exacerbated by 4IR, such as climate change and resource depletion, threaten food security. Global governance efforts must focus on sustainable agricultural practices, equitable distribution, and resilience-building in the face of climate-related disruptions. Health security encompasses access to healthcare, protection against health-related risks, and disease prevention. 4IR has brought about remarkable advancements

in healthcare, including telemedicine, AI-assisted diagnostics, and personalized medicine. These innovations have the potential to improve healthcare access and outcomes globally. However, ethical concerns, data privacy issues, and disparities in access to healthcare technology must be addressed through global governance frameworks to ensure equitable health security for all.

Environmental Security

Environmental security emphasizes the need for a sustainable environment and protection against environmental threats. 4IR technologies can play a pivotal role in monitoring and mitigating environmental risks, such as AI-driven climate modeling and IoT-based environmental monitoring. However, the exponential growth of technology also contributes to electronic waste and energy consumption, impacting environmental sustainability. Global governance mechanisms should prioritize sustainability, regulate harmful practices, and promote responsible technological development. Personal security, which pertains to protection against violence, crime, and human rights abuses, takes on new dimensions in the digital age of 4IR. While advancements in surveillance technology and AI-driven security systems enhance physical security in some contexts, they also raise concerns about privacy infringement and surveillance states. Global governance efforts must strike a balance between ensuring personal security and safeguarding individual privacy and civil liberties.

Community Security

Community security, emphasizing social cohesion and resilience against social disruptions, is integral to human well-being. 4IR technologies can facilitate community building and disaster preparedness through digital communication and information sharing. However, the digital divide and the spread of disinformation pose challenges to community security. Global governance frameworks should work to bridge the digital divide and combat the spread of harmful misinformation.

Political Security

Political security involves the protection of basic human rights, political freedoms, and participation in decision-making processes. In the era of 4IR, political security takes on new dimensions, with concerns about the impact of digital technologies on democracy, freedom of speech, and electoral processes. Ensuring political security in the digital age requires robust global governance mechanisms that safeguard democratic principles, combat cyber threats, and protect the integrity of political systems.

In this multifaceted discussion, we have explored how the Fourth Industrial Revolution intersects with the dimensions of human security and global governance. While 4IR presents unprecedented opportunities for advancement, it

also introduces complex challenges that transcend borders and require collaborative global solutions. The role of global governance is paramount in addressing these challenges, fostering equitable access to technological benefits, and upholding the principles of human security in our rapidly evolving world. As we navigate this transformative era, a comprehensive approach to human security and adaptive global governance will be key to shaping a future that prioritizes the well-being and dignity of all individuals and communities.

Bibliography

Barreto, M. B., & Allis, T. 2019. The Fourth Industrial Revolution: Issues and Implications for Global Governance. *Journal of Globalization Studies*, 10(2): 1–17.

Czempiel, E.-O. 2007. Rethinking Global Governance: A Multidisciplinary Approach. *International Studies Quarterly*, 51(4): 871–881.

Duffield, M. 2007. *Global Governance and the New Wars*. London & New York: Zed Books.

Global Governance and the Emergence of Global Institutions for the 21st Century. 2020. Ed. by A. Lopez-Claros. A. L. Dahl, M. Groff. Cambridge: Cambridge University Press.

Mahbubani, K. 2018. *Has the West Lost It? A Provocation*. New York: Penguin.

Paris, R. 2001. Human Security: Paradigm Shift or Hot Air? *International Security*, 26(2): 87–102.

Schwab, K. 2017. *The Fourth Industrial Revolution*. New York: Crown Business.

Sen, A. 1999. *Development as Freedom*. New York: Alfred A. Knop

Tadjbakhsh, S., & Chenoy, A. M. (Eds.) 2007. *Human Security: Approaches and Challenges*. London: Routledge.

United Nations. n.d. https://www.un.org/

United Nations Development Programme (UNDP). 1994. *World Development Report: New Dimensions of Human Security*.

World Bank. n.d. https://www.worldbank.org/

World Economic Forum. n.d. (Various years). *Reports on the Fourth Industrial Revolution and Globalization*.

Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

3 Cyber Espionage and Cyber Interference—A New Way of Intervening in Another State's Affairs

Patrick C. R. Terry

Cyber Espionage

In recent years, there has been an increasing number of major instances of cyber espionage. Cyber espionage is comparatively risk-free in comparison to other, more traditional forms of espionage. In the past, states were forced to send spies abroad in order to steal documents or bribe foreign government officials in an attempt to procure such documents. The sending state, of course, risked its spies' arrest and subsequent exposure with all the negative consequences for its international relations. Cyber espionage, on the other hand, enables a state to conduct its espionage remotely, often from within its own territory so that the risk of a spy's arrest is comparatively low. It also offers a much greater chance of the espionage activity remaining undetected. Groundbreaking in that respect, of course, were the revelations by Edward Snowden in 2013. As the material leaked by Snowden is so extensive, I will focus on only some of the allegations as they relate to Germany. Mainly based on the information provided by this former contractor of the United States' National Security Agency (NSA), there have, for example, been claims that the NSA, often in cooperation with the British security services, was monitoring a wide range of German government communications, from outside Germany, and mainly from inside the United States (Ball & Hopkins, 2013). This seems to have been made possible by programmes such as PRISM, which enable the NSA to monitor internet communications worldwide, not necessarily involving any actions abroad (Beuth & Biermann, 2013). As a result, the NSA was allegedly able to gather 500 million metadata, originating in Germany, within a four-week-period (Rosenbach & Stark, 2015: 233–237). Furthermore, the NSA had apparently been monitoring the telephone conversations of leading German politicians for many years (Zeit Online, 2015). Among other things, WikiLeaks published minutes of a conversation between German Chancellor Merkel and an assistant, which the NSA had recorded (Süddeutsche, 2015). It was also claimed that the NSA had been able to monitor confidential communications originating from within Germany's Foreign Intelligence Service (Der Spiegel, 2015). Furthermore, the USA was accused of being responsible for the installation of spy ware ("Regin") on a computer used by an assistant working

DOI: 10.4324/9781003633204-4

in the office of the German Chancellor (Zeit Online, 2014). Generally, it seems likely that the NSA and British intelligence services were able to "unlock encryption" that "protect[s] emails, banking and medical information" (Ball et al., 2013). Lastly, it was claimed that the US government was actively "working with tech companies in order to insert weaknesses into products" that could subsequently be exploited by US intelligence agencies (Ball et al., 2013).

Of course, other great powers have been far from inactive as far as cyber espionage is concerned. In 2020, Russia was accused of the so-called Solar Winds hack. SolarWinds is a major technology company located in Texas. Hackers, allegedly from Russia, managed to gain access to the company's software Orion and insert "malicious code" (Jibilian & Canales, 2021). As of March 2020, SolarWinds sent out software updates to its many customers, among them major US government departments, thereby creating a "backdoor" for the hackers to spy on the organizations by installing further malware which enabled the spies to target emails and other data. Up to 18,000 organizations may have been affected, including the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury (Jibilian & Canales, 2021).

Meanwhile, in 2021, China was accused of the so-called Microsoft Exchange hack. Hackers exploited "vulnerabilities" in the Microsoft Exchange email and calendar functions in order to gain access to users' emails as of January 2021. Among the victims were US defence contractors and other US entities. Overall, more than 250,000 users could have been targeted (Novet, 2021). This major event was preceded by another critical cyber espionage incident when it was claimed that China, in 2014, had managed to gain sensitive information on 22.1 million US government employees by the way of "cyber intrusions" targeting the Office of Personnel Management (Sanger, 2015; Nakashima, 2015). At the time, this cyber operation was described as being "among the most potentially damaging cyber heists in US government history because of the abundant detail in the files" (Nakashima, 2015).

Cyber Interference—Elections

Of course, the cyber realm has enabled states to go way beyond data theft, offering them the opportunity to actively intervene in other states' affairs by, for example, meddling in their elections. Here, too, cyber meddling is the preferable course of action. There has always been election meddling, but the risk of exposure for the meddling state was much greater. Agents had to be sent abroad in order to hand over money to the preferred campaign teams; there had to be clandestine meetings in embassies or consulates; and frequently states had to revert to bribing local journalists. Cyber meddling, on the other hand, offers the opportunity of clandestine intervention. So-called 'false-flag' activities in social media or campaign financing with the help of cryptocurrencies is much less risky for the intervenor. Lastly, although no case has so far become known, it may be possible to target the organization of an election

by cyber means, such as manipulating the actual election results, changing the register of voters or causing the electoral process itself to collapse, especially in states that enable electronic voting.

The best-known example of election meddling was the alleged Russian meddling in the US presidential election of 2016. In early 2016, the Russian government and other figures associated with the Russian government allegedly began to prepare their campaign of interference. The aim was to defeat the Democratic Party candidate, the former Secretary of State Hilary Clinton, and to support the election of the Republican Party candidate, Donald Trump (Office of the Director of National Intelligence [ODNI], 2017: II, 1–2; US Senate, n.d.: 32; Denton, 2019: 186). According to US authorities, Russia also sought to sow discord among Americans (US Senate, n.d.: 5, 6, 39) and to generally undermine public trust in the US electoral process and system of government (U.S. Department of Justice [DOJ], 2018; US Senate, n.d.: 5–6; Baines & Jones, 2018: 14–15; Denton, 2019: 186).

To achieve this, the Russia-based Internet Research Agency (IRA), which, according to the US government, was "tasked" to do this by the Russian government (US Senate, n.d.: 5, 22–23, 32), bought advertisements supportive of Trump or his policies on social media sites, such as Facebook (US Senate, n.d.: 6–7, 40–41, 44–45; Baines & Jones, 2018: 10). Moreover, in order to achieve their goal, fictitious Facebook (US Senate, n.d.: 7, 45–46; Denton, 2019: 184), Instagram (US Senate, n.d.: 7: 48–50), and Twitter (now X) (US Senate, n.d.: 50–56) accounts were created. Overall, the IRA was allegedly responsible for more than 61,500 posts on Facebook, more than 116,000 posts on Instagram, and more than 10.4 million tweets on Twitter (US Senate, n.d.: 7). In all of these instances, the IRA's authorship was not acknowledged. Rather, the aim was to create the impression that these were messages posted by US citizens (US Senate, n.d.: 7, 45, 46; Denton, 2019: 184). According to one estimate, the Russian-inspired Facebook posts reached 126 million users (US Senate, n.d.: 45; Denton, 2019: 192). Many of these posts were also successful in instigating actual US citizens to take further action, such as forwarding the posts to acquaintances (US Senate, n.d.: 7, 46). The IRA also used its social media presence to promote Trump rallies (US Senate, n.d.: 46–48).

Furthermore, Russia initiated the hacking of email accounts of persons in the leadership of the Democratic Party who were associated with Hilary Clinton (ODNI, 2017: II–III, 2–3; Baines & Jones, 2018: 10). These emails, which were to prove damaging to the Clinton campaign, were subsequently published by WikiLeaks, allegedly in cooperation with Russian government circles (ODNI, 2017: II–III, 2–3). As is well known, the candidate the Russian government is supposed to have supported, Donald Trump, was victorious in the 2016 presidential election. In his research on election meddling, Dov Levin has concluded that Russian interference may well have been decisive in securing that outcome (Levin, 2020: 229–243).

Russia has been accused of further instances of election meddling, also carried out by cyber means. For example, some have accused Russia of

intervening in the UK's Brexit referendum in 2016 (Corera, 2020) and also its general election in 2019 (Kuenssberg, 2020). While the pro-Brexit UK government subsequently refused to investigate claims that Russia interfered during the 2016 Brexit referendum campaign in favor of the "Leave" campaign (Dwyer, 2020), many others agree that such Russian interference took place (Corera, 2020). In addition to other forms of intervention, some researchers claim that more than 150,000 Russia-based Twitter accounts posted messages in favor of Brexit and that as many as 45,000 such messages were posted in the last 48 hours of the campaign (Mostrous et al., 2017). According to a working paper for the National Bureau of Economic Research, the campaign on Twitter alone may have been sufficient to win the referendum for those who wanted to leave the European Union (EU) (Gorodnichenko et al., 2018: 19). In November 2017, UK Prime Minister Theresa May, without mentioning the Brexit referendum, claimed Russia was "meddling in elections," "weaponis[ing] information," and "plant[ing] fake [news] stories" in order to "sow discord in the West and undermine our institutions" (May, 2017).

Similarly, during France's presidential election campaign in 2017, Russia allegedly hacked and leaked nine gigabytes of data belonging to Emmanuel Macron's campaign team in order to damage his campaign (Greenberg, 2017; Baines & Jones, 2018: 15; Schmitt, 2018: 37). The leak occurred two days before the decisive second round of the election and was mixed with forgeries (Conley, 2018: 1). Nevertheless, this interference proved unsuccessful, as Emmanuel Macron was elected president. As early as February 2017, the French government had warned about interference in France's election: "We will not accept any interference whatsoever in our electoral process. … This is a question of our democracy, our sovereignty, our national independence" (Reuters, 2017).

In the run-up to the parliamentary election in Germany in September 2021, both Germany and the EU accused Russia of trying to interfere (Deutsche Welle, 2021; Der Spiegel, 2021). The German government claimed that Russian intelligence services had been engaged in cyber espionage against German parliamentarians in order to obtain confidential information that the Russian government would then use to launch a campaign of disinformation during the election campaign (Deutsche Welle, 2021). The German government described the Russian behavior as "completely unacceptable" and as a "danger … to the democratic decision-making process" (Deutsche Welle, 2021). The EU concurred with the German government's assessment, "strongly denounc[ing] these malicious cyber activities" and "urg[ing] the Russian Federation to adhere to the norms of responsible state behavior in cyberspace" (Cook, 2021).

Furthermore, US intelligence asserts that Russia once more intervened in the 2020 US presidential election in a similar fashion as had occurred in 2016 in an effort to undermine Joe Biden's candidacy (National Intelligence Council, 2021: i). In response, in April 2021, President Biden imposed sanctions on Russia. In doing so, President Biden emphasized that elections were "sovereign undertakings," as well as an "expression of the will of the American people."

Therefore, the United States could not "allow a foreign power to interfere in our … democratic process with impunity" (Biden, 2021).

Needless to say, other states have surely exploited the internet in a similar way in order to secure a favorable election outcome in another state. Perhaps unsurprisingly, the United States has also frequently been accused of intervening in foreign elections. Massive interventions in Italy's 1948 (Weiner, 2006; US Senate, 1976, Book 1, 49) and subsequent (Pike Report, 1992: xiii; Peck, 2017) elections were accompanied by many such instances in Latin and South America (US Senate, 1975 [Chile]; Bello & Hermann, 1984; Meyer, 1983 (both El Salvador); Marker, 1990; Levin, 2020: 163 [both Nicaragua]). Since the end of the Cold War, the United States has been accused of intervening in Russia's presidential elections of 1996 (Schmitt, 2018: 38; Strickland, 2020; Levin, 2016: 198 fn. 37), its parliamentary elections of 2011 (Strickland, 2020; Bridge, 2011), and the Serbian elections of 2000 (Shimer, 2020). Although most of these interventions date from the pre-cyber era, there can be no doubt that such meddling would now take place utilizing the opportunities the cyber sphere offers.

Prohibited Interventions—A Legal Assessment

Given the far-reaching consequences just outlined, it comes as no surprise that the activities just outlined, cyber espionage and cyber meddling, are frequently unlawful under public international law as they violate the prohibition on interventions in the other state's *domaine réservé*.

Customary international law prohibits interventions in other states' internal affairs (International Court of Justice [ICJ], Corfu Channel 1949: 34–35; Military and Paramilitary Activities 1986a: 202; see also: Armed Activities on the Territory of the Congo 2005: 161–165). The 1970 General Assembly's (GA) 1970 Friendly Relations Declaration reaffirmed that "no State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State" (UNGA Res. 2625 (XXV) 1970). Although GA resolutions are not legally binding, this particular one passed by consensus and explicitly referred to international law, which makes it reasonable to conclude that States viewed it as reflecting international legal rules. In 1986b, the ICJ confirmed that the text of the Friendly Relations Resolution "expresses an *opinio juris*" and "may be understood as an acceptance of the validity of the rule or the set of rules declared by the resolution […]" (ICJ, Military and Paramilitary Activities, 1986a: 188; see also: Armed Activities on the Territory of the Congo 2005: 161–165). The ICJ itself has also repeatedly stressed the legal status of the prohibition of such interventions; as soon as 1949, the Court declared interventions in other states' affairs to be unlawful (ICJ, Corfu Channel, 1949: 34–35).

The ICJ's, 1986a Judgment in the *Nicaragua* Case is frequently cited when discussing the prohibition of interventions, because the court provided a partial definition of its scope. Reaffirming the principle of non-intervention as a

rule of customary international law (Military and Paramilitary Activities 1986b: 202; see also: Armed Activities on the Territory of the Congo 2005: 161–165), the ICJ went on to define a prohibited intervention:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.
>
> (ICJ, Military and Paramilitary Activities, 1986a: 205)

Thus, unlawful intervention consists of two elements. The intervenor must be targeting another State's internal or external affairs or, as the ICJ phrased it, "matters in which each state is permitted … to decide freely" (ICJ, Military and Paramilitary Activities, 1986a: 205; Jamnejad & Wood, 2009: 347). These matters are often referred to as the *domaine réservé* (Helal, 2019: 4), which, as the ICJ explained, includes, "the choice of a political, economic, social and cultural system and the formulation of foreign policy" (ICJ, Military and Paramilitary Activities, 1986b: 205). However, not every State activity in respect of another State's internal affairs is unlawful. Rather, the intervenor must employ "methods of coercion" to achieve its aims (Helal, 2019: 4).

There is disagreement on the definition of the term "coercion" in international law (Helal, 2019: 3, 48, 55). Some claim the ICJ's reference to "methods of coercion" limits the scope of the prohibition of interventions (Ronzitti, 2015: 3; Fatouros, 1976: 192–193; Helal, 2019: 56–57; see generally Jamnejad & Wood, 2009). According to this view, intervention is only prohibited when the level of coercion is comparable to the threat to use force (Ronzitti, 2015: 3; Fatouros, 1976: 192–193). This becomes obvious when some claim that coercive intervention must be "dictatorial" in nature, leaving the target State with no room for manoeuvre (ICJ, Military and Paramilitary Activities, 1986a; Judge Schwebel: 98; Ronzitti, 2015: 3; Fatouros, 1976: 192–193; Helal, 2019: 56–57).

This very limited view of prohibited interventions is more than questionable (Helal, 2019: 75–76; Nunn, 1984: 149–150). Rather, an intervention is unlawful when the aim is to deprive the target State of its discretion to decide freely on issues related to its internal and/or external affairs (Helal, 2019: 71–72). As DeWitt Dickinson indicated as early as 1920, intervention is prohibited when it "cannot be terminated at the pleasure of the State that is subject to the intervention" (DeWitt Dickinson, 2019: 260). Coercion thus merely requires the target state to be unable to respond to the outside interference and therefore forced to tolerate it, irrespective of whether this is due to inability or lack of awareness. In both cases, the target state does not have the ability to defend itself against foreign meddling in its affairs. Equating prohibited intervention

with dictatorial interference is unconvincing, if the prohibition on outside interventions is to have any meaning.

Some claim that a State can only be coerced if it is aware of the intervenor's activities and thus aware of being coerced by it (Tallinn Manual 2.0., 2017). This excludes from the prohibition all activities by the intervening State of which the target State is unaware. This, too, is an unnecessary and unconvincing limitation of the principle of non-intervention (Kilovaty, 2019: 89; Rotondo & Salvati, 2019: 212; Tsagourias, 2019; Tallinn Manual 2.0, 2017). Applied to the US activities in Nicaragua, this would imply that the US support of the *contras* —who were rebelling against the Nicaraguan government—would have been lawful as long as Nicaragua was unaware of American activities and continued to blame the *contras*' activities solely on this domestic opponent, as the principle of non-intervention only applies between states and not between a state's government and its domestic opponents (Tallinn Manual, 2017: 313–314). On the other hand, such activities would become unlawful when the target State became aware of the foreign intervenor's involvement. This unsatisfactory distinction between lawful and unlawful activities evidences that awareness on the part of the target State is not a suitable criterion to differentiate between lawful activities and unlawful coercion and does not reflect extant law (Kilovaty, 2019; Rotondo & Salvati, 2019; Tsagourias, 2019; Tallinn Manual 2.0, 2017). This was also confirmed by the ICJ in the *Nicaragua Case*: despite the "secrecy which surrounded" the financial assistance the US provided the *contras* with, the ICJ did not hesitate to classify this financial support as a prohibited intervention (ICJMilitary and Paramilitary Activities, 1986a: 57, 107, 242). *Opinio juris* also confirm this: both the USA and the UK have declared that manipulating election results by cyber means is an unlawful intervention in the target State's internal affairs (Nye Jr., 2020; Wright, 2018). This view is widely supported (Efrony & Shany, 2018: 641–643) and is incompatible with the view that a State must be aware of the coercion for the intervention to be unlawful.

I will now proceed to apply these basic concepts to cyber interference and cyber espionage, beginning with the former due to such activities potentially far-reaching consequences.

a.) Cyber Interference—Elections

Elections determine a people's "choice of a political, economic, social and cultural system, and the formulation of foreign policy", a decision which, according to the ICJ, must remain free (ICJ, Military and Paramilitary Activities, 1986b: 205). There is, therefore, wide-spread agreement that a state's electoral process is a matter within a state's *domaine réservé* that is protected by the prohibition on interventions (Helal, 2019: 65–67; Barela, 2017; Denton, 2019; Wheatley, 2020: 174; Tsagourias, 2019: 10; Schmitt, 2018: 49; Tallinn Manual 2.0: 315; see also: ICJ, Military and Paramilitary Activities, 1986b: 257–259). This is confirmed by numerous General Assembly resolutions that have stated that

> Any activities that attempt, directly or indirectly, to interfere in the free development of national electoral processes, in particular in the developing countries, or that are intended to sway the results of such processes, violate the spirit and letter of the principles established in the Charter and in the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations.
>
> UN Docs. A/RES/44/147 (1989); A/RES/4 5/1 51 (1990); A/RES/46/130 (1991); A/RES/47/130 (1992); A/RES/48/124 (1993); A/RES/50/172 (1995); A/Res/52/119 (1997); A/RES/ 54/168 (1999); A/RES/49/180 (1995); A/Res/56/154 (2001))

Furthermore, the fact intervenors often seem to succeed in influencing target state election results (Levin, 2020: 5, 7, 38–45, 175–180, 186–187, 246), thereby securing for themselves a say in choosing a target state's government, renders any contrary arguments unconvincing. As Ray Meyer has pointed out, if successful, such an intervention can result in "an inherently more extensive intervention in internal affairs because it may involve an indirect intervention in all future policy decisions made by the tainted government" (Meyer, 1983: 111).

However, the fact that prohibited intervention demands a coercive element means that not every kind of interference by a state in another state's election campaign is unlawful. As long as the interfering state's intent is to persuade, rather than to coerce, meddling activities can be lawful. Thus, open criticism of a political party or government in another state, even during an election campaign, may be seen as an unfriendly act, but it is nevertheless lawful. The targets of such criticism can respond, and the voters in the target state can make their own assessment on how to respond to such foreign interference. Similarly, the online spreading of true information can usually be qualified as lawful interference.

Such lawful meddling turns into prohibited intervention when deception is deployed in order to increase the interference's effectiveness. For example, the posting of political views in social media under the guise of being a target state citizen is unlawful (Helal, 2019: 9; Nunn, 1984: 163; Xiao, 2020: 374 [false identities]; Wheatley, 2020: 190–192 [false identities]). This kind of deceit leaves the target state defenseless against the foreign intervention. It cannot terminate it "at its pleasure" since target state citizens or journalists are well within their rights when expressing their views publicly (Rotondo & Salvati, 2019: 211–212). Furthermore, voters in the target state are misled into believing that these are views put forward by fellow citizens and almost certainly will pay more attention to such opinions than they would to easily identifiable foreign interference (Helal, 2019: 115; Wheatley, 2020: 190–192; Schmitt, 2018: 51). The intervenor's activities, in truth, amount to nothing else but a secret election campaign in support of the preferred candidates. The strategy on the part of the intervening state demonstrates the coercive intent—it chooses to hide the origin of

the views expressed in print, on air or online, in order to deceive the target state and its voters and to prevent the target state from responding (Kilovaty, 2018: 154; Rotondo & Salvati, 2019: 211–212). The coercion towards the target state manifests itself in the intervening state's active participation in another state's election campaign, conducted in a way which the target state cannot prevent or terminate (Terry, 2022). As Dov Levin has concluded, "a covert intervention carries far lower chances of a backlash due to the inherent secrecy in the provision of the electoral aid" (Levin, 2020: 40). An overt intervention, on the other hand, may "lead to a backlash against the preferred candidate, hurting rather than helping their chances of being elected" (Levin, 2020: 40).

If the intervenor's aim is not only to secure the preferred election outcome, but also to undermine public trust in the electoral process more generally, as claimed in the case of the Russian meddling in the 2016 US election (Barela, 2017), the coercive intent becomes even more obvious. The intervenor is seeking to subvert the target state's system of government by way of deception which renders the target state defenseless as long as the deception is not uncovered (Kilovaty, 2018: 156). Should, on the other hand, the deception be uncovered, the public may well view an election outcome as illegitimate—in the belief foreign meddling influenced the results—which undermines the public's trust in its government and is therefore similarly subversive (Barela, 2017; Xiao, 2020: 366).

It is obvious that more serious activities, such as spreading fake news or forging documents that are posted online in order to influence the target state's election outcome, are clearly unlawful (Tallinn Manual, 2013: 45; Helal, 2019: 9, 118; Jamnejad & Wood, 2009: 374; Koh, 2017: 450; Pirker, 2013: 201; supportive: Forcese, 2016). Although spreading disinformation may possibly lead to a target state response, the intervenor's intention is to avoid an effective target state reaction and to deceive that state's electorate.

As far as the spreading of true information gained by way of espionage is concerned, this, too, constitutes unlawful intervention (Tsagourias, 2019: 16). Illicitly gained information (Forcese, 2016; Helal, 2019: 113–114) is instrumentalized in order to influence the target state's election results in a meaningful way. The fact the information was gained by way of espionage taints the dissemination of the information. Based on the intervenor's intent to manipulate the outcome of the election and to therefore intervene in the target state's internal affairs by using the material obtained by deceit and manipulation causes the act of espionage to be unlawful (Helal, 2019: 114; Tsagourias, 2019: 18–19; Terry, 2018: 623). Here, too, the target state is not able to terminate either the espionage or the subsequent dissemination of the information which makes such actions coercive in nature (Hamilton, 2017: 196).

The most severe kind of intervention in the sphere of election meddling is, of course, the manipulation of the electoral process itself (Nye Jr., 2020; Wright, 2018; Efrony & Shany, 2018: 641–643; Levin, 2020: 257–264; Wheatley, 2020: 185–186). Changing election results, making ballots disappear, deleting or adding names to the electoral register or manipulating electronic voting

machines, the "electoral doomsday scenario" (Levin, 2020: 257), are undoubtedly coercive in nature (Nye Jr., 2020; Wright, 2018; Tallinn Manual 2.0: 312; Efrony & Shany, 2018: 641–643; Wheatley, 2020: 185–186; Tsagourias, 2019: 10–11; Schmitt, 2020: 561; Gill, 2013: 234). The target state is not meant to notice the manipulation and is therefore unable to terminate the intervention and the manipulation. If successful, this might well lead to the imposition of a government by outsiders, irrespective of the electorate's wishes. Short of the use of force, this amounts to the most coercive intrusion into another state's electoral process (Terry, 2022).

b.) Cyber Espionage

As far as cyber espionage is concerned, the legal situation is not quite as clear-cut. This is due to the fact that, on the face of it, the coercive element necessary under public international law for an intervention to be unlawful seems to be lacking. On closer examination, however, it turns out that many cyber espionage operations are undertaken in order to enable an unlawful intervention. Thus the spying State's motives when engaging in espionage activities are of great importance when determining whether such actions are lawful (Falk, 1962: 58; Pert, 2013: 2; Shull, 2013: 5; Gehrlein, 1996: 101; Kilovaty, 2016: 70–77). Suppose cyber espionage is carried out to enable the State to undermine the target State's foreign, trade, or domestic policies, i.e., to coercively intervene in the target State's *domaine réservé*. In that case, the act of espionage must be viewed as initiating this unlawful conduct.

This means that cyber espionage activities are unlawful if they are deployed to achieve an unlawful goal (Terry, 2025). Even Asaf Lubin—who views peacetime espionage as a generally lawful activity (Lubin, 2020)—acknowledges this correlation:

> [I]f a specific act of espionage is a constitutive element in a larger wrongdoing, if it is an integral and indispensable element in a chain of events unequivocally leading to the commissioning of an internationally wrongful act, to a point where one cannot conceive of the wrongful activity without imagining the intelligence gathering that necessarily came before it, and if such intelligence was gathered with knowledge of and intent to commit that wrongful activity, then that act of espionage must be deemed unlawful.
>
> (Lubin, 2020: 239)

For example, speaking in hypotheticals, former NSA Director Michael Hayden suggested that it may have been justified to spy on former German Chancellor Gerhard Schröder during his term of office due to his disagreement with US policies surrounding the Iraq war and regarding Russia (Hujer & Stark, 2014). It follows that the material gained, by whatever means of espionage, would have been used to undermine or even thwart Germany's diverging policies. Cyber espionage deployed to obtain information that serves to disrupt another State's foreign policy is then the initiation of an unlawful, coercive intervention.

The UK's former Attorney-General, Suella Braverman, gave examples of what the UK would view as a prohibited intervention by cyber means, namely the "restrict[ion] or prevent[ion] [of] the provision of essential medical services" (Braverman, 2022). Cyber espionage undertaken to gain the necessary information for such actions would then itself obviously be unlawful.

The truth is that cyber espionage often is not a random search for any information that can be found. Rather, cyber espionage is frequently deployed to achieve a specific goal. For instance, in the run-up to the Iraq War in 2003, a leaked memorandum instructed senior members of the NSA to spy on the diplomats of other UN Security Council member States. They were advised that the NSA was "mounting a surge" aimed at gleaning information not only on how delegations on the Security Council will vote on any second resolution on Iraq, but also "policies", "negotiating positions", "alliances" and "dependencies", in short to obtain the "whole gamut of information that could give US policymakers an edge in obtaining results favourable to US goals or to head off surprises" (Bright et al., 2003). In this case, the USA was attempting to collect information so as to be able to flip other states' votes in the Security Council on a matter of grave importance.

Cyber espionage in such instances is clearly undertaken to enable an unlawful intervention in the target State's protected *domaine réservé*, namely its foreign policy, and is, therefore, itself unlawful. The spying State's goal of ultimately intervening in another State's affairs is vital when assessing the lawfulness of the cyber espionage activity deployed towards this goal (Pert, 2013: 2; Stein & Marauhn, 2000: 24; Falk, 1962: 58; Kilovaty, 2016: 70–77). Of course, cyber espionage also enables States to target other States' officials by, for example, intercepting their private email communications and subsequently bribing or blackmailing them (Gehrlein, 1996: 101) in order to secretly pull the strings necessary to change the target State's policies. Whenever cyber espionage is deployed to achieve such aims, the act of espionage itself is unlawful (Terry, 2025).

Cyber interference and cyber espionage are therefore frequently unlawful (Terry, 2022, 2025). If uncovered, such operations may well induce the target state to impose sanctions and/or take other countermeasures against the intervenor which, of course, always carries the risk of escalation.

Conclusion

In this chapter I have outlined how the cyber realm has massively changed the ways in which states spy on each other and meddle in each other's affairs. I have described some of the major cases of cyber espionage and election meddling that have occurred in the last decade. We can safely assume that there have been many more, probably spectacular cases we have not been informed about. The internet and cyber technology have seemingly offered states the opportunity of unlawful, but apparently risk-free interventions abroad. Certainly, the risk of exposure is much lower than in the past when spies had to move about

within the target state, potentially risking arrest, or when it was much more difficult to keep election interference secret because it was extremely challenging to hide the whole range of activities necessary in order to influence an election outcome.

As I subsequently explained, the use of cyber tools to undertake such interventions makes them no less unlawful. And that is where the risk of cyber tools starts to get into focus: it is the seemingly low risk of getting caught and being exposed that may encourage states to intervene much more often and perhaps more forcefully in the expectation of being able to maintain deniability should the operation be exposed after all. The more states feel encouraged to intervene in other states' affairs, however, the more likely it becomes that such operations will be exposed. The more massive and successful such an intervention turns out to be, the more forceful the response by the other state will be. The risk of escalation is obvious. It is therefore in states' interest to (1) invest heavily in cyber security in order to deter and defeat such attempts at cyber intervention by other states, and (2) to begin international negotiations in order to create rules that govern cyber conduct. Such negotiations are urgently needed, as the danger of massive interventions in foreign elections is growing rapidly due to the vast possibilities the internet offers. As Dov Levin has pointed out, the greatest dangers to the integrity of future elections are massive campaign funding utilizing cryptocurrencies (Levin, 2020: 253–257) and tampering with election results (Levin, 2020: 257–264). Furthermore, as seen in the recent Argentinian presidential elections, which have been described as the "[f]irst A.I. [e]lection" (Nikas & Herrera, 2023), the vast opportunities artificial intelligence (AI) offers to manipulate content in combination with the methods of cyber meddling described above could potentially lead to a situation in which voters can no longer distinguish between fact and fiction when heading to the polls. The same is true of cyber espionage. As we have seen in the past, most spectacularly during the Iraq Crisis in 2002/2003, intelligence agencies can usually uncover only a part of the truth as far as other states' intentions, defence capabilities, etc. are concerned—the risk of a state acting on such partial information should not be underestimated, potentially leading to catastrophe. Negotiations on binding rules for the cyber realm should therefore be initiated, but conducted on a level playing field (Lahmann, 2020: 222–223). More recent attempts by some states to proceed on the basis of exceptionalism, however, will undoubtedly fail.

References

Baines, P. & Jones, N. 2018. Influence and interference in foreign elections: The evolution of its practice. *Royal United Services Institute Journal*, 163(1): 12–19.

Ball, J., Borger, J. & Greenwald, G. 2013, September 6. Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Ball, J. & Hopkins, N. 2013, December 20. GCHQ, NSA targeted charities, Germans, Israeli PM and EU chief. *The Guardian*. http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

Barela, S. J. 2017, January 12. Cross-border cyber ops to erode legitimacy: An act of coercion. *Just Security*. https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/

Bello, W. & Hermann, E. S. 1984. US-sponsored elections in El Salvador and the Philippines. *World Policy Journal*, 1: 851–869.

Biden, J. 2021, April 15. *Remarks on Russia at the Presidential Briefing Room*. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/15/remarks-by-president-biden-on-russia/

Beuth, P. & Biermann, K. 2013, June 17. Das spionage-system prism und seine Brüder. *Zeit Online*. http://www.zeit.de/digital/datenschutz/2013-06/nsa-prism-faq

Braverman, S. 2022, May 19. Speech: International law in future frontiers. *UK Government*. www.gov.uk/government/speeches/international-law-in-future-frontiers

Bridge, R. 2011, December 9. Election-Meddling Fiasco Hits US–Russia relations. *RT*. https://www.rt.com/russia/russia-us-elections-clinton-putin-2012-usaid-427/

Bright, M., Vulliamy, E. & Beaumont, P. 2003, March 2. Revealed: US dirty tricks to win vote on Iraq war. *The Guardian*. www.theguardian.com/world/2003/mar/02/usa.iraq

Conley, H. A. 2018, June 21. Introduction. In *Successfully Countering Russian Electoral Interference*, edited by H. A. Conley & J.-B. J. Vilmer. Center for Strategic & International Studies. Briefs. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Cook, L. 2021, September 24. EU warns Russia over cyberattacks ahead of German elections. *Associated Press News*. https://apnews.com/article/technology-russia-elections-media-foreign-policy-a9abb7e00e4430c402b07ae14cdd9c8c

Corera, G. 2020, October 29. MPs and peers demand Russia interference inquiry. *BBC*. https://www.bbc.com/news/uk-politics-54725758

Denton, A. 2019. Fake news: The legality of the Russian 2016 Facebook influence campaign. *Boston University International Law Journal*, 37: 183–210.

Der Spiegel 2015, September 25. *Snowden-Dokumente: NSA fing offenbar BND-Kommunikation ab*. http://www.spiegel.de/netzwelt/netzpolitik/fairview-nsa-hat-sensible-informationen-des-bnd-abgefangen-a-1054727.html

Der Spiegel 2021, September 24. *EU Wirft Russland vor Bundestagswahl Gezielte Cyberangriffe vor*. https://www.spiegel.de/netzwelt/netzpolitik/eu-wirft-russland-vor-bundestagswahl-gezielte-cyberangriffe-vor-a-9ee768d4-007a-418c-9bdc-f99e4cd590b0

Deutsche Welle. 2021, September 6. *Bundesregierung Fordert von Russland Ende der Cyberattacken*. https://www.dw.com/de/bundesregierung-fordert-von-russland-ende-der-cyberattacken/a-59100108

DeWitt Dickinson, E. 1920/2019. *The Equality of States in International Law*. Harvard University Press.

Dwyer, C. 2020, July 21. U.K. "actively avoided" investigating Russian interference, lawmakers find. *NPR*. https://www.npr.org/2020/07/21/893443735/u-k-actively-avoided-investigating-russian-interference-lawmakers-find?t=1633619533235

Efrony, D. & Shany, Y. 2018. A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, 112(4): 583–657.

Falk, R. A. 1962. Space espionage and world order: A consideration of the Samos-Midas-Program. In *Essays on Espionage and International Law*, edited by Roland J. Stanger, 45–82. Columbus: Ohio State University Press.

Fatouros, A. A. 1976. Covert intervention and international law. *Maurer Faculty Paper 1890*. https://core.ac.uk/download/pdf/232668746.pdf

Forcese, C. 2016, December 16. The "hacked" US election: Is international law silent, faced with the clatter of Cyrillic keyboards? *Just Security*. https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards

Gehrlein, M. 1996. *Die Strafbarkeit der Ost-Spione auf dem Prüfstand des Verfassungs- und Völkerrechts*. Heymann.
Gill, T. D. 2013. Non-intervention in the cyber context. In *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, 217–238. NATO CCD COE.
Gorodnichenko, Y., Pham, T. & Talavera, O. 2018. Social media, sentiment and public opinions: Evidence from #BREXIT and #USELECTION. *National Bureau of Economic Research*. Working Paper No. 24631. https://www.nber.org/system/files/working_papers/w24631/w24631.pdf
Greenberg, A. 2017, May 9. The NSA confirms it: Russia hacked French election "infrastructure". *WIRED*. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/
Hamilton, L. 2017. Beyond ballot-stuffing: Current gaps in international law regarding foreign state hacking to influence a foreign election. *Wisconsin International Law Journal*, 35: 179–204.
Helal, M. S. 2019. On coercion in international law. *New York University Journal of International Law and Politics*, 52(1): 1–122.
Hujer, M. & Stark, H. 2014, March 24. Shame on us. *Der Spiegel*. www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389.html
International Court of Justice (ICJ). 1949. *Corfu Channel* (United Kingdom v. Albania). ICJ Rep. 4.
International Court of Justice (ICJ). 1986a. *Military and Paramilitary Activities* (Nicaragua v. United States). ICJ Rep. 14.
International Court of Justice (ICJ). 1986b. *Military and Paramilitary Activities* (Nicaragua v. United States). Dissenting Opinion Judge Schwebel. ICJ Rep. 14.
International Court of Justice (ICJ). 2005. *Armed Activities on the Territory of the Congo* (Dem. Rep. of Congo v. Uganda). ICJ Rep. 168.
Jamnejad, M. & Wood, M. 2009. The principle of non-intervention. *Leiden Journal of International Law*, 22(2): 345–381.
Jibilian, I. & Canales, K. 2021, April 15. The US is readying sanctions against Russia over the Solar Winds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. *Business Insider*. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
Kilovaty, I. 2016. World wide web of exploitations—The case of peacetime cyber espionage operations under international law: Towards a contextual approach. *Columbia Science and Technology Law Review*, 18: 42–78.
Kilovaty, I. 2018. Doxfare: Politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information. *Harvard National Security Journal*, 9: 146–179.
Kilovaty, I. 2019. The elephant in the room: Coercion. *AJIL Unbound*, 113: 87–91.
Koh, H. H. 2017. The Trump administration and international law. *Washburn Law Journal*, 56: 413–469.
Kuenssberg, L. 2020, July 16. "Almost Certain" Russians sought to interfere in 2019 UK election—Raab. *BBC*. https://www.bbc.com/news/uk-politics-53433523
Lahmann, H. 2020. Information operations and the question of illegitimate interference under international law. *Israel Law Review*, 53: 189–224.
Levin, D. H. 2016. When the great power gets a vote: The effects of great power electoral interventions on election results. *International Studies Quarterly*, 60: 189–202.
Levin, D. H. 2020. *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*. Oxford University Press.
Lubin, A. 2020. The liberty to spy. *Harvard International Law Journal*, 61: 185–243.

Marker, D. 1990, February 14. A catalog of constant US interference. *The Christian Science Monitor*. https://www.csmonitor.com/1990/0214/emark.html

May, T. 2017, November 13. *PM Speech to the Lord Mayor's Banquet 2017*. https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017

Meyer, R. 1983. The limits of intervention in the political process: The role of the United States in El Salvador. *ASILS International Law Journal*, 7: 89–123.

Mostrous, A., Bridge, M. & Gibbons, K. 2017, November 15. Russia used Twitter Bots and Trolls "to disrupt" Brexit Vote. *The Times*. https://www.thetimes.co.uk/article/russia-used-web-posts-to-disrupt-brexit-vote-h9nv5zg6c

Nakashima, E. 2015, July 9. Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.319beab5403b

National Intelligence Council. 2021. *Intelligence Community Assessment No. 2020-00078D*. Foreign Threats to the 2020 US Federal Elections.

Nikas, J. & Herrera, L. C. 2023, November 15; updated November 16. Is Argentina the First A.I. Election. *The New York Times*. https://www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html

Novet, J. 2021, March 9. Microsoft's big email hack: what happened, who did it, and why it matters. *CNBC*. www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html

Nunn, K. B. 1984. Legality of covert action under contemporary international law. *Berkeley La Raza Law Journal*, 1: 139–167.

Nye, Jr., P. C. 2020, March 2. *DOD General Counsel Remarks at US Cyber Command Legal Conference*. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

Office of the Director of National Intelligence. 2017, January 6. *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment. https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf

Peck, M. 2017, February 12. Declassified: How America planned to invade Italy (To Save It from Russia). *The National Interest*. https://nationalinterest.org/blog/the-buzz/declassified-how-america-planned-invade-italy-save-it-russia-19401

Pert, A. 2013, November 27. Australia's Jakarta phone-tapping: was it illegal? *Inside Story*. https://insidestory.org.au/australias-jakarta-phone-tapping-was-it-illegal/

Pirker, B. 2013. Territorial sovereignty and integrity and the challenges of cyberspace. In *Peacetime Regime for State Activities in Cyberspace*, edited by Katharina Ziolkowski, 189–216. Tallinn: NATO CCD COE.

Reuters. 2017, February 15. *France Warns Russia against Meddling in Election*. https://www.reuters.com/article/us-france-election-cyber-idUSKBN15U22U

Ronzitti, N. 2015. Respect for sovereignty, use of force and the principle of non-intervention in the internal affairs of other states. *European Leadership Network*. https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/ELN-Narratives-Conference-Ronzitti.pdf

Rosenbach, M. & Stark, H. 2015. *Der NSA Komplex*. München: Wilhelm Goldmann Verlag.

Rotondo, A. & Salvati, P. 2019. Fake news, (dis)information, and the principle of non-intervention. *The Cyber Defense Review*, Special Edition: 209–224.

Sanger, D. E. 2015, September 6. Cyberthreats confound US. *International New York Times*, *1*.

Schmitt, M. N. 2018. "Virtual" disenfranchisement: Cyber election meddling in the grey zones of international law. *Chicago Journal of International Law*, 19(1): 30–67.

Schmitt, M. N. 2020. Autonomous cyber capabilities and the international law of sovereignty and intervention. *International Law Studies*, 96: 549–576.

Shimer, D. 2020, June 21. When the CIA interferes in foreign elections. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2020-06-21/cia-interferes-foreign-elections

Shull, A. 2013. Cyberespionage and international law. *Paper presented at the GigaNet 8th Annual Symposium SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809828

Stein, T. & Marauhn, T. 2000. Völkerrechtliche Aspekte von Informationsoperationen. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 60: 1–40.

Strickland, D. 2020. Overriding democracy: American intervention in Yeltsin's 1996 reelection campaign. *Footnotes, a Journal of History*, 4: 166–181.

Süddeutsche Zeitung. 2015, July 2. *NSA-Abhörprotokolle von Angela Merkel*. http://www.sueddeutsche.de/politik/spionage-nsa-abhoerprotokoll-von-angela-merkel-1.2547431

Tallinn Manual on the Law Applicable to Cyber Warfare 2013. Edited by Michael N. Schmitt. CUP.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2017. Edited by Michael N. Schmitt & Liis Vihul. CUP. 2nd ed.

Terry, P. C. R. 2018. "Don't do as I do"—The US response to Russian and Chinese cyber espionage and public international law. *German Law Journal*, *19*: 613–626.

Terry, Patrick C. R. 2022. Voting by proxy- meddling in foreign elections and public international law. *Indiana Journal of Global Legal Studies* 29: 69–117

Terry, Patrick C. R. 2025. *Peacetime Cyber Espionage and International Law in Research Handbook on Intelligence and International Law*, edited by Russell Buchan and Iñaki Navarrete. Edward Elgar Publishing, 353–376.

The Unexpurgated Pike Report. 1976/1992. *Report of the House Select Committee on Intelligence*, edited by Gregory Andrade Diamond. McGraw-Hill, Inc.

Tsagourias, N. 2019. Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace. *White Rose Research Online*. http://eprints.whiterose.ac.uk/159652/

United Nations. 1970. General Assembly Resolution 2625 (XXV).

United Nations. 1989. Respect for the Principles of National Sovereignty and Non-interference in the Internal Affairs of States in Electoral Processes, UN Docs. A/RES/44/147.

United Nations. 1990. A/RES/45/151. (1991) A/RES/46/130. (1992) A/RES/47/130. (1993) A/RES/48/124.

United Nations. 1995. A/RES/49/180. (1995) A/RES/50/172. (1997) A/RES/52/119.

United Nations. 1999. A/RES/54/168.

United Nations. 2001. Respect for the Principles of National Sovereignty and Non-interference in the Internal Affairs of States in Electoral Processes as an Important Element for the Promotion and Protection of Human Rights, UN Doc. A/Res/56/154.

US Department of Justice. 2018, February 16. Grand Jury Indicts Thirteen Russian Individuals and Three Companies for Schemes to Interfere in the United States Political System. *Press Release*. https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

US Senate. 1975. 94th Congress, 1st Session, Covert Action in Chile 1963–1973, Staff Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. https://www.intelligence.senate.gov/sites/default/files/94chile.pdf

US Senate. 1976. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee"), Final Report. Senate Report No. 94–755, Book 1.

US Senate. n.d. 116th Congress, 1st Session, (U) Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and

Interference in the 2016 US Election, Volume 2: Russia's Use of Social Media with Additional Views, Report 116-XX. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Weiner, T. 2006, July 6. F. Mark Wyatt, 86, C.I.A. Officer, Is Dead. *The New York Times*. https://www.nytimes.com/2006/07/06/us/06wyatt.html

Wheatley, S. 2020. Foreign interference in elections under the non-intervention principle: We need to talk about "coercion". *Duke Journal of Comparative & International Law*, 31: 161–197.

Wright, J. 2018, May 23. *Cyber and International Law in the 21st Century*. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

Xiao, A. 2020. Responding to election meddling in the cyberspace: An international law case study on the Russian interference in the 2016 presidential election. *Duke Journal of Comparative & International Law*, 30: 349–378.

Zeit Online. 2014, December 29. *Spionagesoftware auf Computer im Kanzleramt*. https://www.zeit.de/digital/2014-12/virus-spionage-kanzleramt

Zeit Online. 2015, July 2. *Regierung bestellt US-Botschafter ein*. http://www.zeit.de/politik/deutschland/2015-07/nsa-merkel-spionage-wikileaks

4 Israel's Techno-Nationalism

Technology, Identity, and Geopolitics

Manjari Singh

Introduction

As a phenomenon, techno-nationalism emerged during the industrial era, when it was pursued by leading nations such as Britain, Germany and the United States as they sought to strengthen their national economies through the promotion of domestic industries. By introducing policies such as protectionism, industrial espionage and government-sponsored research, these nations asserted their superiority. In today's geopolitical landscape, techno-nationalism has emerged as a nationalistic and ideological framework aimed at understanding how technological advancements shape the social and cultural fabric of a nation and influence its citizens. As a fusion of "technology" and "nationalism", it is politically focused on the advancement of a nation in terms of technology and its related dynamics.

As a formalized concept, techno-nationalism is a modern phenomenon rooted in the 19th-century period of industrialization and state-led technological development. However, in a broader historical perspective, elements of techno-nationalist thinking could have been present in the ancient and classical civilizations, as each civilization sought a technological supremacy for power, security and economic advantage. This ranges from advanced urban planning and the development of the sewage system, through knowledge of metallurgy to the developed agricultural techniques in the Indus Valley civilization and the advanced irrigation system and engineering techniques used in the building pyramids and medical knowledge during the Mesopotamian and Egyptian civilizations.

Greek and Roman technological identity in mathematics, science, architecture, early mechanical devices such as the Antikythera mechanism, and the construction of engineering marvels in the form of aqueducts etc. are among the examples of the achievements of these civilizations, which are valued even today. These advancements were certainly aimed at gaining advantage over the adversary, even though the modern concept of the nation-state did not exist at that point in time. Similarly, in Jewish literature the mention of the Ark of the Covenant as a symbol of national identity, military power and religious supremacy cannot be ignored. The Torah and other biblical texts

DOI: 10.4324/9781003633204-5

contain numerous references to technological advancements, craftsmanship, divine knowledge, technological exclusivity.

As described in Exodus 25–31, the Tabernacle or *Mishkan* was a state-commissioned mobile sanctuary, constructed with highly detailed specifications—evoking parallels with modern-day, state-guarded strategic installations in military and industrial domains. Likewise, Genesis 11:1–9 describes the construction of the Tower of Babel, where humanity unites to build a tower to reach the heavens. This was intended to highlight the dangers of uncontrolled technological advancement, a can be seen as akin to the restrictions on modern technology transfer between competing nations. Solomon's Temple and Philistine Iron monopolization are other examples of the technological prowess of the time.

In the modern sphere of international relations, techno-nationalism has been defined at various lengths, oscillating between being an ideology, a strategic approach, a policy or a concept which nations adopt to integrate technological advancement to their national security. Each of the definitions places an emphasis on technological control, national security, and economic strategy, which are the key pillars of techno-nationalism. While there are varied definitions of the term, among the most widely accepted ones and relevant to Israel's case are those advanced by Andrew B. Kennedy and Darren J. Lim (2018), Alex Capri (2020) and Robert D. Atkinson (2020).

Andrew Kennedy and Darren Lim (2018) define techno-nationalism as:

> A form of economic nationalism that links a nation's technological capabilities and industrial base to its national security, economic competitiveness, and geopolitical influence. It involves policies that support domestic technological innovation while restricting foreign access to critical technologies.
>
> (Kennedy and Lim, 2018: 554)

Atkinson defines techno-nationalism as an "idea that a nation's economic and national security depend on its ability to develop, produce, and control key advanced technologies" (Atkinson, 2020: 23). In contrast, Alex Capri defines techno-nationalism as a "new strain of mercantilist thinking that links technological innovation and capabilities to a nation's national security, economic prosperity and social stability" (Capri, 2020: 4). In short, modern observers see techno-nationalism, broadly defined, as a policy framework or ideology that links technological innovation and industrial capability to national security, economic prosperity, and global influence. It emphasizes state-led initiatives to develop, protect, and control critical technologies for strategic advantages.

In the context of Israel, techno-nationalism lies at the intersection of technological advancement and national identity, which has become a defining feature of Israel's existence and development as a state. The Jewish state's strategic prioritization of technology stems from both necessity and ambition: Necessity to survive amidst adverse conditions at the time of its independence; and ambition to be recognised by nation-states as a worthwhile strategic partner. It is

additionally driven by security concerns, economic aspirations and global geopolitical positioning.

Given this necessity, Israel's techno-nationalism is deeply rooted in its historical resurgence as a nation-state. Since its founding in May 1948, and even before that time, the country has pursued technological self-reliance owing to its limited natural resources and regional hostilities. The establishment of the Kibbutz system played a crucial role in not only enabling early Jewish settlers to cultivate crops in the arid lands of Greater Palestine in the late 19th and early 20th centuries, but also integrating cutting-edge agri-tech solutions, which could serve as models for sustainable farming. Israel's advancements in agricultural technology, including precision farming, drip irrigation, and desert agriculture, have made Kibbutzim key hubs for agricultural innovation (Singh, 2023). Over a period of time, the Kibbutzim became not just a communal agricultural settlements but also an early experiment in using technology to overcome environmental constraints, ensuring self-sufficiency and later being developed as the first line of civilian defence against Hamas and Hezbollah.

If this were not sufficient, Israel transformed its identity from being a pioneer in military technologies to becoming a global leader in cybersecurity and artificial intelligence. From developing cutting-edge defensive technologies such as the Iron Dome system, Merkava tanks and unmanned aerial vehicles (UAVs) (Kober, 2007), to building nuclear and space capabilities through the development of Dimona Nuclear Reactor and establishing Israel Aerospace Industries (IAI) (Cohen, 2010), to normalizing relations with Arab Gulf nations through cybersecurity and AI and the development of water and agricultural technologies (Norlen & Sinai, 2020), Israel has efficiently used technology to establish its national aspirations. It leveraged its technological prowess as simultaneously a defensive, political and economic asset. Its technological advantage ensured the country's survival in a hostile region and at the same time it facilitated its diplomatic outreach and its normalization with a number of Arab states and also played a decisive role in establishing partnerships with countries such as India. This chapter aims to examine the historical, military, economic, and geopolitical dimensions of Israel's techno-nationalism and analyses its implications for global power dynamics.

Historical Foundations of Israel's Techno-Nationalism

Israel's emergence as a techno-nationalist nation is deeply rooted in its history wherein the narrative of the Kibbutz movement played a pivotal role in fostering innovation and in establishing institutions that have contributed to the country's technological progress. The concept can be traced back to the late 19th and early 20th centuries, coinciding with the rise of Zionism, the Jewish nationalist movement (Grossman, 2012). With the emphasis on self-reliance and modernization, the movement embraced technological advancement to establish a self-sustaining and secure nation-state.

Collective technological adoption became the ethos of Kibbutzim. They preferred a technological and scientific approach over traditional subsistence farming as the goal was to grow high-yielding nutrient-rich crops to feed its population, along with the faster production of food on largely infertile land. The Kibbutz model, which was introduced in 1909 with the founding of *Degania Alef*, became the nucleus of these efforts.

To overcome the obstacles of the arid and infertile land of Palestine, the early Zionist settlers adopted innovative agricultural techniques and thus this period saw the establishment of various agricultural institutions, training farms and even a Ministry of Agriculture. This ministry was one of the first to be established, with Aharon Zisling becoming its first minister on 14 May 1948, the day of Israel's independence (Singh, 2023: 8). Given the Kibbutzim functioned as collective enterprises, they enabled large-scale investments in infrastructure and research and this led to the mechanization of agriculture (meaning that the use of modern tractors, plows and automated irrigation methods could be efficient), scientific agricultural research (many Kibbutzim collaborated with research institutions and private enterprises to develop drought-resistant crops), and the adoption of hydroponics, greenhouses and controlled-environment farming.

While the Kibbutzim were collective communities established primarily on the basis of agriculture, many of these also ventured into industrial sectors, and set up factories and production units. Over time, these industries diversified into textiles, metal work, and plastics, contributing significantly to Israel's industrial structure. From contributing to national security and addressing regional hostilities by serving as fortified settlements and by making barren lands cultivable, the Kibbutzim helped to strengthen Jewish claims over land. In addition to advancements in high-tech agriculture, Israel simultaneously established the foundations of a robust startup ecosystem and deep military-industrial linkages, further reinforcing its innovation-driven growth model. Notably, many Kibbutz-born engineers and scientists contributed to Israel's tech boom. Likewise, technologies developed in these communal settlements influenced both the defence and water management sectors.

In the current times, the Kibbutzim have evolved and embraced high-tech industries. For instance, Kibbutz Hatzerim, which founded Netafim in 1965, revolutionized water usage in agriculture globally through drip irrigation technology. Likewise, Kibbutz Sasa developed Plasa, which went on to become a leading manufacturer of vehicle armor systems. Through such initiatives, the Kibbutzim evolved as centers of innovations in Israel, a role that they continue to play significantly (Solomon, 2017). Collaborative efforts owing to the communal ethos of Kibbutzim facilitated the use of resources and funds pooled for educational programmes, vocational centers, research initiatives, and the establishment of technological incubators. Through these initiatives, it was possible for Israel to invest in long-term projects in partnership with academic institutions and private enterprises and thereby to train skilled professionals to foster further innovation.

Organizations such as *Startup Nation Central* have been instrumental in establishing technology incubators within the Kibbutz to attract startups and initiate in innovations. Along with the diversification of the Kibbutzim economic base, such initiatives also aim to integrate them to the broader national and global technological landscape. As of January 2025, under the Israeli Innovation Authority's Incubators Incentive Programme, there are about 16 incubators in various fields which are focused on transforming innovative ideas into viable businesses by providing early-stage startups with funding, mentorship, office space. and administrative support (Startup Nation Central, 2025). These incubators are diversified and are involved in various sectors, namely:

- Food Tech: *The Kitchen Hub*, *Fresh Start*.
- Health Tech: *eHealth Ventures*, *AION Labs*
- Climate Tech: *NetZero Tech Ventures*
- Agtech: *Trendlines*, *InNegev*
- Defence Tech and Cyber Incubators: *Incubit Ventures*, *The Defense Hub*, *SOSA Ventures*, *Innofense*
- Broad Focus Incubators: *FinSec Innovation Lab*, *Nielsen Innovate*, *BizTEC*, *Technological Innovation Incubators Program*, *Labs/02*.

When it comes to the intersection of Israel's Kibbutz-based innovation culture and its military-technological prowess, the cooperative communal settlements served not only as defensive outposts but also as makeshift weapon manufacturing sites. Kibbutz-driven military innovation was first observed during Israel's War of Independence in 1948. In another instance, Kibbutz Degania played a critical role in the production of arms and manufacturing of mortars and grenades during the war (Segey, 1998). Given that, since its inception, Israel has faced existential security threats owing to its geographical vulnerability and resource constraints, and therefore technological ingenuity, to gain a qualitative edge was the only reliable solution. In that context, early improvisations provided by Kibbutzim laid the groundwork for the development of Israel's indigenous industrial defence complex.

The Kibbutzim continued to contribute to Israel's military-industrial complex in the decades following the country's independence, to the extent that leading defence companies such as Rafael Advanced Defense Systems, Israel Aerospace Industries and Elbit Systems were inspired and influenced by the Kibbutz-style of problem-solving skills to missile defence and precision-guided weaponry (Kober, 2008). Even the Israeli military, through its elite technology units such as *Unit 8200*, have drawn heavily on the Kibbutzim ingenuity and adaptability required for high-tech military operations, and has created a pipeline of technologically adept individuals who were absorbed into these units (Senor & Singer, 2009). Thus, it is safe to say that Israel's technological development and innovation is deeply rooted and shaped by its socio-economic realities, security concerns and national ethos (Katz, 2018). In the process, Kibbutzim have been significant contributors through their collective community model

which has played a pivotal role in Israel's early nation-building efforts. In addition to their agricultural pursuits, Kibbutzim fostered a conducive environment for innovation in the fields of military technology and defence industries.

Israel's High-Tech Ecosystem: Technology, Innovation and Artificial Intelligence

According to a study conducted by Susann Schäfer and Sebastian Henn (2023), based on the outcome of the development path, Israel's high-tech ecosystem can be classified into three distinct stages: *pre-emergence*, *emergence* and *growth of the entrepreneurial ecosystem*. Each of these phases is marked by specific migration dynamics. *Pre-emergence*, or the first stage (1970–1989), is characterized by the remigration of high-skilled Israelis or the "New Argonauts" (Saxenian, 2007) from the US, including those who had worked in the Silicon Valley. This population might have migrated either because of their love for their homeland and the birthright status provided to Jews in Israel or for patriotic reasons. The migrants possessed outstanding professional acumen in the US and hence could successfully establish and promote transnational connections. They utilized their acquired knowledge to build technology startups in Israel. They were absorbed in high-tech industries as leading entrepreneurs and R&D scientists and were able to channel their professional connections for funds and investors in the US and Europe. This was one of the first instances in whuch foreign investors gained footholds in the emerging Israeli high-tech ecosystem (Aharoni, 2009). While the numbers of these "New Argonauts" was comparatively small, they were a catalyst in terms of playing a role in connecting Israel's emerging high-tech industry with foreign markets as well as in initiating outreach for the vibrant entrepreneurial ecosystem, which led to many investors, managers and incubators being interested in the sector.

Emergence of entrepreneurial ecosystem, the second stage (1990–2007), is marked by the in-migration of Jews from the diaspora. The main driver behind this wave of in-migration was economic opportunity, particularly spurred by the rapid growth of Israel's high-tech industry. This phase is also characterized as the "sunshine migration" (Kenney, Breznitz and Murphree, 2013). It was analysed that this group of migrants were better educated and skilled than those who decided to stay in the US (Cohen & Haberfeld, 2001). Similar to the New Argonauts, there is strong empirical evidence to suggest that, as a result of their high skill levels, this strand of migrants contributed significantly to Israel's high-tech industry as investors, accelerator managers and university professors (Menipaz et al., 2011).

Israel's *growth of entrepreneurial ecosystem*, or third stage, has taken off since 2008 given the number of start-ups, domestic and foreign accelerators and the magnitude of foreign investments, and the number of corporate deals (Finder, Start-Up Nation, 2017). This is the phase which has seen a massive export of Israel's high-tech firms to the Middle East region as well as in the wider world. The phase has been amplified by the growing demand for Israeli

technology in the outside world which has led to the country's global recognition as a technological giant. The massive internationalization of Israeli technology has led to the country being able to create its Silicon Valley equivalent, Silicon Wadi.

Israel has emerged as a global leader in technology owing to its "Start-Up Nation" status (Senor & Singer, 2009), given its remarkable innovatory and entrepreneurial spirit. The country ranks first in the world in terms of the number of startups per capita, in R&D expenditures as a percent of GDP, in venture capital investments per capita, and in unicorns per capita (Gochnour, 2022). This transformation is rooted in a combination of factors such as increased investments in R&D (US$25.2 billion), a highly educated and skilled workforce (51 percent of the population between 25 and 64 have tertiary attainment; 400,000 salaried employees in Israel worked in high-tech companies in 2023), and a culture that fosters innovation (9,093 companies in 2023). The sector contributes 18 per cent to the country's GDP (Statista Research Department, 2025; OECD, 2024; Israel Innovation Authority, 2024). Given all these factors, it is no surprise that in 2024 the Jewish state ranked 15th of 133 countries on the Global Innovation Index (GII) as estimated by the World Intellectual Property Organization (WIPO), while it ranks first in the West Asia and North Africa region (WIPO, 2024). Additionally, Tel Aviv has been recognised as a leading tech hub and has secured 4th position after Silicon Valley, New York and London in Startup Genome's annual ranking of global tech ecosystems, thus underscoring its dynamic startup environment (Wrobel, 2024). Its lose connection to the Israel Defence Force (IDF) and the vision of majority startups to attain global stature since the onset are striking features of the Israeli entrepreneurial ecosystem (Cavusgil & Knight, 2015). Moreover, Israel's ability to quickly adapt to shifting dynamics has made its high-tech sector remarkably agile and resilient. For instance, there has been a phenomenal surge in adapting and increasing the country's capacity to develop cutting-edge technologies that address global challenges.

In this context, the cybersecurity sector, which is driven by increasing demand for cloud and artificial intelligence security solutions, cannot be ignored. According to a *Reuters* report, in 2024 alone, Israeli cybersecurity firms, primarily through a global venture capital firm YL Ventures, raised US$4 billion. This suggests that cybersecurity is becoming a fast-growing segment in Israel's high-tech sector, which, in itself, is a key economic growth driver, accounting for 20 percent of economic activities, 16 percent of job creations and more than half of the country's exports (Scheer, 2025). It is noteworthy that, despite regional geopolitical instability, the nation's cybersecurity influence is expanding sharply to the extent that Israeli cybersecurity startups are emerging as dominant global market leaders.

While the close connection to Israel's defence industry is essentially responsible for the rise of its high-tech entrepreneurial ecosystem, deep intertwining with its military advancement creates a unique growth synergy for both the sectors. The seamless integration of innovation and defence has not only

strengthened Israel's security architecture but also helped position the country as a global leader in technological advancement. Since its independence in May 1948, Israel has tightly bound its technology and national security, which has resulted in creating innovative and highly effective defence infrastructure. This unique relation and synergy between the two distinct sectors coming together and forming Israel's military-technology industrial complex is instrumental in crafting advanced defence systems and has placed the country at the top of the global defence technology market (Vohra, 2023).

The establishment of a Directorate of Defense Research and Development (DDR&D) within Israel's Ministry of Defence is a mark of such a collaboration. The directorate serves as a globally recognised centre of knowledge and expertise in military technology, and contributes significantly to the development, production and maintenance of tools and technologies used by IDF and the defence establishment. By maintaining a qualitative military edge, the directorate ensures the protection of its population. The Ministry of Defense webpage highlights the responsibilities of DDR&D in terms of developing innovative concepts for defence technology, to manage the ministry's short- and long-term development projects, to cooperate with international partners and private sectors for R&D, to serve as a professional, technical body for R&D in military and defensive technology, and, finally, to train the next generation of personnel and tech experts in the country's defence establishment.

The Military Research and Development Unit within DDR&D initiates and leads technological projects, focusing on the areas of missile systems, UAVs and cyber capabilities. This is the unit that collaborates with academic institutions, research centres, high-tech companies and defence industries to combine technologies and develop solutions that address operational gaps. Deep military-technical synergy with several Western countries, primarily the US, further strengthens Israel's defence-industrial complex. Crucial technological inputs are included in such collaborations to both Western and non-Western weapons platforms which is responsible for Israel exerting a significant influence in the global defence market despite its relatively small size (Bommakanti, 2023). A joint partnership between the US-based Raytheon and Israel's Rafael Advanced Defense Systems is one notable example of such international collaborations in developing David's Sling Air Defence system. This partnership is a classic example of the fusion of Israeli innovation with international defence capabilities, resulting in advanced systems that enhance global security (Lye, 2019). In another such development, IAI and India's Defence Research and Development Organization (DRDO) have co-developed a medium-range surface-to-air-missile (MRSAM) named the BARAK 8 Air defence system (Singh, 2022).

Integrating artificial intelligence in its advanced technologies, especially those in defence applications, has become a hallmark of Israel's military-technology complex. The country has incorporated AI into cybersecurity and autonomous systems with precision and thus made its innovations highly effective. This fusion of AI and defence has not only upscaled its national

security aspect, but also propelled it to the top of the global defence technology market (Aravantinos, 2024).

Once again, advancements in AI-driven applications within the Israeli context has been made possible because of strong synergy between the IDF, its intelligence agencies (Mossad and Shin Bet), and its private sectors. The IDF, and its intelligence unit Unit 8200, work closely with leading defence firms such as Rafael Advanced Defense Systems, Elbit Systems and IAI to develop cutting-edge technologies (Bergman, 2022). Given this collective ecosystem, Israel has deployed AI across a wide range of military domains, including its autonomous weapons, in cyber warfare, and in its operational decision-making. However, an overdependence on AI-driven technologies with limited human interventions led to its criticism in the recent Israel–Hamas war (Singh, 2024).

Most notable areas of AI integration are autonomous weapons and precision targeting, such as in Hermes and Heron drones, as well as loitering munitions like Harop. These utilize AI for real-time target identification and engagement (Singer, 2009). AI-powered missile defence systems, such as the Iron Dome, David's Sling, and Arrow, have significantly advanced and enhanced interception accuracy and have optimized response times (Kahana, 2020). Similarly, the Scorpius electronic warfare system employs AI to detect and neutralize electronic threats across multiple domains, thereby reinforcing the country's supremacy in electronic warfare (IAI, 2022).

When it comes to cyber warfare and intelligence, once again AI plays a critical role in Israel's national security strategy. AI is leveraged for advanced signal intelligence (SIGINT), predictive threat analysis and in building a cyber defence mechanism (Singer & Friedman, 2014). Even open-source intelligence (OSINT) uses AI-driven tools to monitor terrorist activities, detecting emerging threats and enhancing cybersecurity resilience. Battle management systems such as Fire Weaver allow real-time data integration to optimize battlefield decision-making and to increase operational efficiency and precision (Elbit Systems, 2021). AI-powered facial recognition, surveillance drones, and big data analytics are applied to identify threats and automate risk assessments in complex urban environments. Thus, the successful installation of AI-driven military applications has led to their frequent usage in urban warfare and in counter-terrorism and counter-insurgency operations (Bergman, 2022).

Such integration is helpful for the defence forces in terms of analysing terrorist networks and predicting potential attacks with greater accuracy. Conscription in the country's defence forces allows the soldiers to gain experience in cybersecurity and AI-driven defence technologies; some of these officials are absorbed into the private sector upon the completion of their compulsory military service. This enables them to be updated in such technologies and thus helps in fostering a culture of innovation and rapid technological development (Senor & Singer, 2009).

In recent conflicts, including the response to the October 7 attack by Hamas, Israeli companies such as Xtend have developed advanced indoor drones which are capable of high-precision strikes with minimal human intervention and are

used by the Israeli army. This is one of the reasons why Israeli defence ministry has fast-tracked numerous startups to support its war efforts. Such instance application of advanced technology in the face of a conflict reflects the level if innovation employed by the country (Rose, 2025). Furthermore, international tech giants have deepened their ties during war times. For instance, during the Gaza War of 2023, Microsoft extended its relations with the Israeli military, increasing its supplies of cloud computing and AI services through the Azure platform. This indicates the growing involvement of private sector tech companies in military operations and how they play an integral role in defining the decisive nature of modern warfare (Davies & Abraham, 2025).

Given Israel's active investment in AI-driven hypersonic missile tracking, quantum AI for encryption and cybersecurity, and swarm AI drones for enhanced combat operations, it is certain that with sustained government and private sector involvement, the country is focused on remaining at the forefront of AI-powered military innovation. At one level, this strengthens national security; on another, it propels Israel towards becoming a leading exporter of defence technology and thus preparing itself to remain relevant for the future of AI warfare (Kahana, 2023).

Leveraging Technological Advancements for Normalization and Regional Cooperation

Given that the Middle East region remains one of the most conflict-prone regions in the world due to the proliferation of non-state actors, proxy wars and deep-seated regional rivalries, Israel is compelled to invest heavily in its military infrastructure. Non-state actors such as Hezbollah, Hamas, the Houthis and various militant factions, often backed by external powers, have significantly shaped the region's security landscape, amplifying the threat of asymmetric warfare, drones and cyber capabilities. Military preparedness is, therefore, crucial, especially for regional powers who have also, more often than not, suffered attacks to their critical infrastructure. Furthermore, geopolitical rivalries have intensified the need for advanced military technologies to counter emerging threats.

In the wake of such threats, while the countries get supported by external actors, such as the US, and have also started to invest in an indigenization process. However, over-reliance on a single actor is a risky business, and therefore countries in the region are moving towards the diversification of their military platforms. In this context, Gulf nations such as the UAE and Saudi Arabia have sought to modernize their defence apparatus with cutting-edge technologies, including AI-driven weapon systems. Most of these options are available outside the region; however, in Israel, the countries have found a cheaper regional alternative. Moreover, as the country advances in its military technology, along with water management and civilian technologies, its presence in the region cannot be ignored. Israeli military-technology firms, known for their expertise in advanced surveillance, missile defence, cyber warfare and AI-powered

unmanned vehicles, present an attractive option. But this requires recognition and the normalization of relations between the Arabs and the Israelis. The *Abraham Accords* facilitated such cooperation between the regional players. While military cooperation and partnerships have not yet, been explored, they may be a future possibility.

Israel's technological prowess serving as a key instrument has enabled the country to build, normalize, and enhance its relations with neighbouring Arab nations, including the Gulf States. The nexus between military technology, startup innovation, and water management technologies such as drip irrigation and desalination, have played a crucial role in this aspect. These advancements have not only contributed to better strategic positioning in the region but also helped Israel to gain global recognition as a nation-state. Given the complexities of the Palestinian issue at hand and the constant threat to its national security from non-state actors such as Hamas, Hezbollah and, most recently, the Houthis, recognition is what Israel aspires for most.

Through the development of sophisticated military hardware, cyber security solutions and intelligence-sharing mechanisms, Israel has made attractive partners with Gulf countries. Through the *Abraham Accords*, the UAE and Bahrain seek closer ties with Israel in a range of areas, a security infrastructure will also follow in the times to come (Vakil & Quilliam, 2023). The accord provides potential for defence cooperation, including access to Israel's Iron Dome missile defence system and advanced cybersecurity capabilities. Technologies in countering drone warfare, cyber espionage and intelligence analysis have the potential to attract the Gulf States' attention towards Israel (Khorrami, 2021).

In addition to military technology, other technological innovations in Israel and the acceleration of its "Start-up Nation" status has the potential to attract the Gulf nations significantly as these countries are aiming towards economic diversification beyond hydrocarbons. The Gulf States have shown their interest in Israel's artificial intelligence, fintech, smart cities ventures and are looking forward to joint ventures in bilateral, trilateral and minilateral formats (Senor & Singer, 2009). At present, Israeli companies have expanded their footprints in Dubai's financial and tech sectors and some Gulf-based venture capital firms are investing in Israeli startups. The UAE–Israel Business Council, launched in 2020 in the aftermath of the Abraham Accords, has facilitated numerous collaborations in multiple sectors ranging from clean energy to digital healthcare (Bauer, 2022).

Israel's expertise in water management has emerged as a significant driver of diplomatic engagement with the Gulf nations. By using groundbreaking technologies such as desalination, wastewater recycling, and drip irrigation, Israel has been able to transform an arid landscape into a thriving agricultural sector and the water-deprived arid Arab nations are very interested in collaborating on these aspects (Tal, 2018). In recent years, Israel has signed agreements with the UAE and Bahrain to collaborate on sustainable water solutions. The UAE and Israel have even initiated joint research projects on improving desalination

efficiency and managing agricultural water use in extreme climates (Rabinovich and Strenberg, 2020). Although formal diplomatic normalization between Israel and Saudi Arabia has not yet occurred, both Riyadh and Abu Dhabi—countries that rely on imports for nearly 90 percent of their food supply—have shown growing interest in adopting Israeli innovations in water conservation, particularly drip irrigation, to strengthen their domestic food production and enhance long-term food security.(Pebbles, 2021).

Thus, the Abraham Accords can be viewed as a watershed moment in breaking longstanding diplomatic barriers between Israel and the Arab world. Furthermore, Israel's expanding economic and technological partnerships have positioned it as a key player in global innovation networks. This recognition from Gulf Arab countries is crucial for Israel and has encouraged other nations to reevaluate their diplomatic stance towards Israel. Indonesia is a good example of this. These initiatives have also enhanced Israel's global recognition as a leader in innovation and technology, and its ability to work in transregional format. I2U2 and the India–Middle East–Europe Economic Corridor (IMEC) are the best examples in this regard. With a flourishing of cooperation in trade, defence, technology and scientific innovations, Israel has been successful in leveraging these aspects in building, and sometimes bolstering, its relations and has managed to elevate its global influence and has reinforced its status as a technological powerhouse.

To conclude, Israel's adoption of techno-nationalism has been instrumental in shaping its national identity, its economic growth and its geopolitical standing. Kibbutzim, communal and cooperative settlements, have played a monumental role in improving the agility of Israel's technological progress. The proverb *Necessity is the mother of invention* is aptly suited to define the country's techno-nationalism. Starting off with agricultural advancement techniques employed for sustenance, Israel's technological history has seen a sea-change. By leveraging cutting-edge defence and civilian technology, the Jewish nation has positioned itself as a key global innovator.

The country's advancement in military technology, startups, cybersecurity and AI-powered developments, water management, and other developments, have been pivotal in reshaping its relations in the region, especially with the Arab and Gulf Arab nations. A convergence of interests in the domains of security concerns, economic interests, clean energy, and sustainable initiatives has fostered a pragmatic approach to regional cooperation amplified by the Abraham Accords. These initiatives have not only normalized and strengthened Israel's diplomatic stature in the wider Middle East region but also enhanced its global recognition as a leader in innovation and technology and its ability to work in transregional format. Continued expansion of such collaborations is likely to shape the future of the Middle East, demonstrating the country's ability to channel technology-driven diplomacy. As the global landscape evolves, Israel's ability to sustain its technological edge while balancing its diplomatic and security concerns will determine its future role.

References

Aharoni, Y. 2009. Israeli multinationals: Competing from a small open economy. In *Emerging Multinationals in Emerging Markets*, edited by R. Ramamurti and J. V. Singh. Cambridge: Cambridge University Press.

Aravantinos, E. 2024. The fusion of technology and defense: Israel's military-technology complex. *Strategy International*, 21 November, available at: https://strategyinternational.org/2024/11/21/publication150/, accessed on 20January2025.

Atkinson, R. D. 2020. The case for a national industrial strategy to counter China's technological rise. *Information Technology and Innovation Foundation (ITIF)*, pp. 1–31.

Israel Innovation Authority. 2024. *2023 Annual Report: The State of High-Tech*. Israeli Central Bureau of Statistics, available at: https://innovationisrael.org.il/files-en/2023-06/2023%20Annual%20Innovation%20Report.pdf, accessed on 25January2025.

Bauer, Katherine 2022. Israel–UAE economic cooperation has deep roots and broad dividends. *The Washington Institute of Near East Policy*, 8 March, available at: https://www.washingtoninstitute.org/policy-analysis/israel-uae-economic-cooperation-has-deep-roots-and-broad-dividends, accessed on 20January2025.

Bergman, R. 2022. *Israel's Intelligence Operations in the Digital Age*. New York: Harper Collins.

Bommakanti, K. 2023. *The Strategic and Military-Technological Significance of Israel*. Observer Research Foundation. Experts Speak: Raisina Debates. New Delhi. 22 December, available at: https://www.orfonline.org/expert-speak/the-strategic-and-military-technological-significance-of-israel/, accessed on 20January2025.

Capri, A. 2020. Techno-nationalism and diplomacy: The US–China race to reshape alliances, institutions and standards. *Hinrich Foundation*, 2020: 4, available at: https://www.hinrichfoundation.com/research/wp/tech/techno-nationalism-and-diplomacy/, accessed on 20January2025.

Cavusgil, S. T. and Knight, G. 2015. The born global firm: An entrepreneurial and capabilities perspective on early and rapid internationalisation. *Journal of International Business Studies*, 46: 3–16.

Cohen, A. 2010. *The Worst Kept Secret: Israel's Bargain with the Bomb*. New York: Columbia University Press.

Cohen, Y. and Haberfeld, Y. 2001. Self-selection and return migration: Israeli-born Jews returning home from the United States during the 1980s. *Population Studies*, 55: 79–91.

Davies, H. and Abraham, Y. 2025. Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war. *The Guardian*, 23 January, available at: https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft, accessed on 30January2025.

Elbit Systems. 2021. *Fire Weaver: AI-Powered Battle Management*, available at: www.elbitsystems.com, accessed on 20January2025.

Finder, Start-Up Nation 2017. *Companies*, available at: https://finder.startupnationcentral.org/, accessed on 20January2025.

Gochnour, N. 2022. What the startup state can learn from startup nation. *Deseret News*, 24 September, available at: https://www.deseret.com/opinion/2022/9/24/23369059/opinion-israel-start-up-nation/#:~:text=In%20meetings%20with%20the%20Israeli,capita%20and%20unicorns%20per%20capita., accessed on 20January2025.

Grossman, D. 2012. *Rural Settlement and Kibbutz in Jewish Palestine: 1882–1948*. Oxford: Oxford University Press.

IAI (2022). *Scorpius: The Future of Electronic Warfare*, available at: www.iai.co.il, accessed on 20January2025.

Kahana, E. 2020. *Israeli Intelligence and the Defense of the Nation*. London: Routledge.

Kahana, E. 2023. *Cybersecurity and Artificial Intelligence in Israeli Defense Strategies*. London: Cambridge University Press.

Katz, Y. 2018. Technology and innovation in Israel: Advancing competitive position in a global environment. *Open Journal of Political Science*, 8: 536–546.
Kennedy, A. B. and Lim, D. J. 2018. The innovation imperative: Technology and US–China rivalry in the twenty-first century. *International Affairs*, 94(3): 553–572.
Kenney, M., Breznitz, D. and Murphree, M. 2013. Coming back home after the sun rises: returnee entrepreneurs and growth of high tech industries. *Research Policy*, 42: 391–407.
Khorrami, N. 2021. One year on—Israel's cybersecurity cooperation with the GCC states. *Middle East Institute-National University of Singapore*, 14 September, available at: https://mei.nus.edu.sg/publication/insight-266-one-year-on-israels-cybersecurity-cooperation-with-the-gcc-states/, accessed on 20January2025.
Kober, A. 2007. From Blitzkrieg to Attrition: Israel's attrition strategy and staying power. *Small Wars & Insurgencies*, 16(2): 216–240.
Kober, A. 2008. *Israel's Defense Doctrine and Military Strategy*. London: Routledge.
Lye, H. 2019. Technology born from the US and Israel's special defence relationship. *Army Technology*, 15 August, available at: https://www.army-technology.com/features/us-israel-defence-technology-relationship/, accessed on 20January2025.
Menipaz, E. A., Yedidsion, Y. and Lerner, M. 2011. *Israel National Entrepreneurship Report*. Ira Center for Business Technology and Society. Ben Gurion University.
Norlen, T. and Sinai, T. 2020. The Abraham Accords—Paradigm shift or realpolitik? *George C. Marshall European Center for Security Studies*, 64, October, available at: https://www.marshallcenter.org/en/publications/security-insights/abraham-accords-paradigm-shift-or-realpolitik, accessed on 20January2025.
OECD. 2024. *Survey of Adults Skills 2023: Israel*, 10 December, available at: https://www.oecd.org/en/publications/survey-of-adults-skills-2023-country-notes_ab4f6b8c-en/israel_3915a641-en.html, accessed on 20January2025.
Pebbles, V. 2021. *Water diplomacy in the Middle East: Israel, Jordan and Palestine*. Ford School, University of Michigan. 8 November, available at: https://fordschool.umich.edu/event/2021/water-diplomacy-middle-east-israel-jordan-and-palestine, accessed on 20January2025.
Rabinovich, I., and Strenberg, Y. 2020. *Water and Diplomacy: Israel's Role in Solving Regional Water Crises*. Tel Aviv: Tel Aviv University Press.
Rose, E. 2025. Israeli startups make global plans after key role in war. *Reuters*, 31 January, available at: https://www.reuters.com/world/middle-east/israeli-startups-make-global-plans-after-key-role-war-2025-01-31/, accessed on 5February2025.
Saxenian, A. L. (2007). *The New Argonauts: Regional Advantage in a Global Economy*. Cambridge: Harvard University Press.
Schäfer, Susann, and Henn, Sebastian 2023. Start-up nation Israel: Transnational entrepreneurs, born globals and cross-border connections of the Israeli high-tech industry. In *Research handbook on transnational diaspora entrepreneurship*, edited by R. Sternberg, M. Elo, J. Levie, and J. E. Amorós (pp. 129–145). Edward Elgar Publishing.
Scheer, S. 2025. Israel cyber firms raise $4 billion in 2024, on surge of cloud, AI security needs. *Reuters*, 7 January, available at: https://www.reuters.com/technology/israel-cyber-firms-raise-4-bln-2024-surge-cloud-ai-security-needs-2025-01-07/#:~:text=JERUSALEM%2C%20Jan%207%20(Reuters),YL%20Ventures%20said%20on%20Tuesday., accessed on 20January2025.
Segey, T. 1998. *1949: The First Israelis*. London: Macmillan Publishers.
Senor, D. and Singer, S. 2009. *Start-Up Nation: The Story of Israel's Economic Miracle*. New York: Twelve Books.
Singer, P. W. 2009. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Books.
Singer, P. W. and Friedman, A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. London: Oxford University Press.

Singh, M. 2022. India-Israel defence relations: From longstanding to robust. *CLAWS Journal*, 15(1): 129–139.

Singh, M. 2023. Agri-tech and Israel. In *The Palgrave International Handbook of Israel*, edited by P. R. Kumaraswamy (pp. 1–17). Singapore: Palgrave Macmillan.

Singh, R. 2024. Unveiling the intelligence gaps: A critical examination of intelligence failure on 7 October Hamas attack. *Strategic Analysis*, 00(00): 1–11.

Solomon, S. 2017. Claiming to be Israel's first start-up ventures, Kibbutzim jump on tech bandwagon. *The Times of Israel*, 31 December, available at: https://www.timesofisrael.com/claiming-to-be-israels-first-startup-ventures-kibbutzim-jump-on-tech-bandwagon/, accessed on 20January2025.

Startup Nation Central. 2025. 16 Israel Incubators to watch in 2025. 12 January, available at: https://startupnationcentral.org/hub/blog/16-israel-incubators-to-watch-in-2025/, accessed on 20January2025.

Statista Research Department. 2025. Total National Expenditure on Civilian Research and Development in Israel from 1996 to 2023. 21 January, available at: https://www.statista.com/statistics/1549419/national-expenditure-on-civilian-research-and-developmentisrael/#:~:text=In%202023%2C%20the%20national%20expenditure, compared%20to%20the%20preceding%20year., accessed on 29January2025.

Tal, A. 2018. *The Land and the Water: Israel's Environmental Challenges and Achievements*. New York: Yale University Press.

Vakil, S. and Quilliam, N. 2023. *The Abraham Accord and Israel–UAE Normalisation: Shaping a New Middle East*. Chatham House. Middle East and North Africa Programme, available at: https://www.chathamhouse.org/sites/default/files/2023-04/2023-03-28-abraham-accords-israel-uae-normalization-vakil-quilliam-1.pdf, accessed on 20January2025.

Vohra, A. 2023. Israel's military-technology complex is one of a kind, *Foreign Policy*, 19 December, available at: https://foreignpolicy.com/2023/12/19/israels-military-technology-complex-is-one-of-a-kind/, accessed on 20January2025.

WIPO. 2024. Israel ranking in the global innovation index 2024. *Global Innovation Index*, available at: https://www.wipo.int/edocs/gii-ranking/2024/il.pdf, accessed on 20January2025.

Wrobel, S. 2024. Tel Aviv moves up to fourth place in annual ranking of global tech ecosystems. *The Times of Israel*, 10 December, available at: https://www.timesofisrael.com/tel-aviv-moves-up-to-4th-place-in-annual-ranking-of-global-tech-ecosystems/, accessed on 20January2025.

5 Taiwan Strait and the Semiconductor Crisis—Its Geopolitical Implications and a Critic to Complex Interdependency Theory

Shalendra D. Sharma and Soumyodeep Deb

Introduction

Taiwan is a significant industry leader thanks to the arrival of the "Fourth Industrial Revolution". This is mostly because of their proficiency in producing semiconductors, which is the most valuable component of this industrial era. Modern digital and technological advancements have been fueled by semiconductors and chips (Tang & Ji, 2023). This is thought to significantly influence the future generation of industries, including defense, electronics, smart computing, automotive, and artificial intelligence. Thus, semiconductors have been argued to propel the modern economy (Palmer, 2023). Because of its firm hold on semiconductor manufacturing, Taiwan has acquired a strategic position in the global economy. It has become a major source of semiconductors. This has led to the dependence of large international corporations on Taiwan for industries such as automotive, defense, electronics, and next-generation technologies (Crawford et al., 2021). Not only are the big Western corporations dependent on Taiwan, but China also imports the majority of its advanced semiconductors from Taiwan. Therefore, it can be argued that China is dependent on Taiwan because the country's semiconductor sector has not yet developed to the same extent. However, the worsening of the cross-strait relations between China and Taiwan has highlighted the supply chain side of the semiconductor industry. China has recently increased its military presence in the Taiwan Strait, reaffirming that the ultimate goal is to unite Taiwan with the mainland. Though the main goal has been to attain this through peaceful means, in recent times, the possibility of using force has also been raised. This demonstrates the unpredictability of cross-strait relations. The global supply chain and geo-economics would be significantly affected if there are any major events around this vicinity. China, which depends on Taiwanese semiconductors, will also be severely impacted. However, other countries are also worried about their own security as semiconductors are currently a critical element of national security. China would escalate the situation if Taiwan raises the question of independence, notwithstanding its dependence on the country for its supply of semiconductors. Consequently, one could argue that security overrides the interdependency in the general dynamics of world politics.

DOI: 10.4324/9781003633204-6

Semiconductors: the Core of 21st-Century Technology

The importance of semiconductors increases as technology dictates power dynamics. Crude oil was the driving force for development and power in the 20th century. The same can be said about semiconductors in the 21st century. Everything, from cars, solar panels, and smartphones to computers and military hardware, contains semiconductor chips. With the world moving towards the development of renewable energy, the significance of semiconductor chips is gaining in importance (Matta, 2023). The processing power of a chip determines the efficiency of the product. With renewable energy being pushed by all major nations, the role of advanced chips would be a linchpin factor in a move towards this direction. Along with renewables, the advent of artificial intelligence (AI) has revolutionized the importance of semiconductor chips. The computing power of modern-day supercomputers depends on the processing power of these chips. With AI being the most important revolution in this era, the power driving the revolution is the semiconductor chips. The military domain is also heavily dependent on the advancement of this technology. Therefore, these components are the driving force for next-generation power domination in the context of the most important technological processes. Given Taiwan's dominance of the manufacturing and supply chain of this critical subject, any geopolitical turmoil will have major global implications (Table 5.1).

Taiwan currently has the largest market share in the semiconductor manufacturing industry. This is mostly because of the actions made in the early years of the Republic of China (ROC) administration. The 1976 agreement with Radio Cooperation of America (RCA) opened the door to Taiwan's success in semiconductor manufacturing (Taiwan Today, 2010), leading to the establishment of the first semiconductor manufacturing plant in Taiwan. As a result of this arrangement, the country could receive RCA semiconductor technology to construct the first 3-inch wafer fabrication plant. Additionally, labor costs in East Asian countries were low, which encouraged Western corporations to relocate their production facilities to Asia. This period saw the rise of Taiwan and Korea as manufacturing hubs, with the US acting as their main market and the US and Japan being the providers of the necessary technology (Hsu, 2017).

Since then, Taiwan has leapfrogged in this sector, becoming a leading semiconductor manufacturer. Taiwan now leads the industry, producing more

Table 5.1 Taiwan's Share in Global Semiconductor Production

Countries	*Production percentage (%)*
Taiwan	68.3
South Korea	8.5
US	6.6
China	7

than 60% of the world's chips and contributing roughly 15% of its GDP (Dimerco, 2023).

Table 5.1 aggregates the percentages of Taiwan's total market control, indicating its position in the global semiconductor supply chain. In addition to being the leading supplier, it also comprises 90% of the most sophisticated semiconductor chips (Dasgupta, 2022). Taiwan is principally responsible for producing the cutting-edge semiconductor chips that power most modern electronics. In the advanced semiconductor segment, the Taiwan Semiconductor Manufacturing Cooperation (TSMC) leads. Presently, it is among the limited firms manufacturing large quantities of 3 nanometer chips, which are at the forefront of semiconductor technology (Wu, 2022). The width between a transistor and a chip is measured in nanometers; the smaller the number, the more transistors that can be incorporated into the chip, increasing its power while also making its manufacturing extremely difficult and expensive (Fang, 2022). Therefore, some of the most cutting-edge tech companies, such as Apple, Nvidia, Qualcomm, AMD, and Intel, are now reliant on TSMC for their chips (Campbell, 2021). However, it is not just leading IT corporations but all other industries which are now reliant on the availability of advanced chips. As a result, both businesses and countries have become reliant on Taiwan, and particularly TSMC, for the advanced processing of powered chips. This situation hit the headlines when TSMC was unable to provide chips to the automotive industry during the COVID epidemic, leading to the global suspension of auto production (Crawford et al., 2021) (Table 5.2).

Moore's law, named after Intel's Gordon Moore, asserts that the number of transistors in a chip doubles every two years. It is considered to be the guiding principle in the semiconductor industry (Gustafson, 2011). Consequently, TSMC is driven to constantly improve its technological prowess and deliver the most cutting-edge processors. As the company continues to follow Moore's law, it plans to develop chips that are two nanometers in size, starting in 2026 (Yahoo Finance, 2023). TSMC will be the first to do this, demonstrating how corporations control the majority of the factors that influence our daily lives. As a result, TSMC has such a stronghold on the chip market that it is governments, rather than other businesses, who are TSMC's competitors, since every country is attempting to improve its capacity for the production of

Table 5.2 Global Companies' Share in Global Semiconductor Production (%)

Company	*%*
TSCM	55.5
Samsung	16
UMC	6.8
Global Founders	5.9
SMIC	5.3

Source: Compiled by authors

semiconductors (Campbell, 2021). Therefore, it is possible to claim that the majority of businesses, despite their efforts to relocate manufacturing to their respective countries, would continue to rely on Taiwan to supply them with the most cutting-edge semiconductor chips, which would be essential to their manufacturing and economic environments.

Given that Taiwan and China are engaged in a long-standing geopolitical struggle, escalating Sino-US tensions also have an impact on cross-strait ties. Beijing promised to reabsorb Taiwan back into its territory because it has long seen it as an essential component of the Chinese nation. This has long been the source of concern that China will use force to bring Taiwan back within its borders, and the growing power disparity strengthens this claim. China has made peaceful reunification a top priority, but it has not held back from declaring that it has the right to use force if it deems it necessary (France 24, 2019). With China's rapid rise and military modernization, this has been a cause of concern in Taiwan. However, as argued by scholars, Taiwan's hold on semiconductor manufacturing provides a defense, called the "silicon shield" (Cronin, 2022). Since Taiwan is a vital supply network for semiconductors, any aggression against it would destroy it, bringing global industry, and even China's economy, to a halt. Scholars have contended, therefore, that Taiwan will have the best deterrence because of its dominance in chip production and global dependency. However, in light of China's increasing military drills and belligerent activities around the Taiwan Strait, this deterrent is now being seriously called into question. In addition, there has been a major push by Beijing to enhance its own semiconductor capabilities with the aim of achieving complete self-reliance in this area. Such a development would bring about a major transformation in the geopolitical situation, as a reduction in China's reliance on Taiwan for high-end semiconductors will increase the possibility of cross-strait military action.

China's Push Towards Self-Reliance in Semiconductors

An improvement in semiconductor production capability has been a major focus of the Chinese government. The semiconductor was one of the major components in China's "Made in China 2025" strategy, in which Beijing wanted to be a global leader. Under this strategy, Beijing has provided massive investments and subsidies in the semiconductor sector with the aim of attaining self-reliance in this production technology (Schumacher, 2024). This led to the establishment of the National Integrated Circuit Industry Investment Fund, better known as the "Big Fund." The core objective of this body was to attract funds from state-owned enterprises, financial institutions, and private investors to build a robust semiconductor ecosystem (Lee, 2024). Phase I of the Big Fund initiative was launched between 2014 and 2019. During the first phase, various investments saw the nurturing of a number of major semiconductor players such as the Semiconductor Manufacturing International Cooperation (SMIC). Phase I of the initiative saw a total investment of

approximately 139 billion yuan ($21.5 billion). This has been fundamentally used to enhance research and build a foundation for the development of the semiconductor industry.

The Big Fund phase II was launched in 2019–2024 and saw a total of 204 billion yuan ($31.63 billion) being allocated. Phase II of the study was more nuanced. This worked to enhance China's semiconductor capability through increased R&D and by integrating the supply chain to move up the value chain. This phase has been argued to be crucial in upholding China's semiconductor sufficiency amid increasing US sanctions (Lee, 2024). Phase II of funding has backed more than 20 projects across various sectors of semiconductor manufacturing to enhance both production and supply chains (Ma, 2023). Compared with Phase I of the initiative, Phase II of the Big Fund saw a much more diverse array of investors, 27 in total. Table 5.3 lists some of the major shareholders of China's Big Fund Phase II scheme (Table 5.3).

Therefore, shareholding is now very scattered, unlike in Phase I (Liu, 2019). This shows that the semiconductor funding initiative has received major traction in China, helping pump more funds to enhance its capabilities. However, the issue of corruption caused a dent in the program in 2022, with the arrest of one of the biggest government fund managers of Sino-IC Capital (Ding et al., 2022).

But this has not stopped Beijing from launching Phase III of the initiative in 2024 with a hefty investment plan of $47.5 billion (Lee, 2024). The duration of the phase has also been extended to 15 years, from May 2024 to May 2039. This initiative aims to work on all segments of semiconductor manufacturing and target pervious bottlenecks to ensure better productivity. For this purpose, the Central Science and Technology Commission was created to oversee the plans and their execution (Mok, 2023). It follows a policy of centralized oversight, which restricts the occurrence of corruption. Therefore, the fund size and aggressive push show that China wants to attain major self-reliance in the field of semiconductor manufacturing in the near future.

Table 5.3 The Big Fund's Stake in Global Semiconductor Companies (%)

Company	*The Big Fund's Stake (%)*
Semiconductor Manufacturing International North China (Beijing) Corp	32
Hua Hong Semiconductor (Wuxi) Ltd	29
Yangtze Memory Technology Holdings Co Ltd	24.1
Unisoc (Shanghai) Technologies Co Ltd	14
Empyrean Technology Co Ltd	8.9
Beijing BDStar Navigation Co Ltd	8.6
NAURA Technology Group Co Ltd	7.5
Advanced Micro-Fabrication Equipment Inc China	4
Goodix Technology Inc	3.6
National Silicon Industry Group Co Ltd	2.7

Source: Compiled by authors from various media sources

It can be argued that China's move towards reliance on semiconductor manufacturing will have direct ramifications on the overall security apparatus of the Taiwan Strait. As China's current share of global chip output is only marginal, its reliance on Taiwan and other Western powers is crucial for its survivability. However, under its goal of semiconductor self-reliance, its level of dependency will be reduced. This would also reduce the significance of Taiwan and other Western powers for China, which, in turn, could embolden its military actions to attain reunification. However, even in the current context, with China being dependent on Taiwan and other powers for its access to chips, its military posture around the Taiwan Strait has only increased.

China's Growing Assertive Push Around Taiwan

The entire security architecture of East Asia has been significantly affected by cross-strait relationships. For China, the island nation of Taiwan is seen as a renegade province that has to be brought under Chinese administration. This has been the PRC's main foreign policy goal since it was founded in 1949. Therefore, China adopted an aggressive foreign policy towards Taiwan from the very beginning, which resulted in significant combat engagements in the 1950s (US Department of State, n.d.). However, when China entered the Deng Xiaoping period, there was an improvement in relations across the Taiwan Strait. This was related to China's new "hide and bide" approach, which, under Deng, became its core foreign policy tenet (Deb, 2023). China's approach to Taiwan was reoriented because of changes in its foreign policy approach. This gave the concept of a one-country, two-system more traction and hastened the idea of peaceful reunification (Liu, 2020).

This approach has recently undergone a significant change as a result of China's assertive ascent. China's cross-strait relations and general international relations have changed significantly since Xi Jinping assumed political leadership. China has recently placed a high priority on the revitalization of the country to realize its dream (Deb, 2023). The fundamental goal of the China Dream is to restore China's stature and prominence in the world by elevating it to the status of a great power. Taiwan serves as this vision's pivotal point, since Chinese people cannot fully recover without reunification. Consequently, the legitimacy of the Chinese Communist Party (CCP) legitimacy would suffer significantly if reunification was not achieved (Culver & Hass, 2021). This poses a serious threat to the party, and thus the Chinese government, as the party controls the government in China.

Additionally, the Democratic Progressive Party's (DPP) ascent to power in Taiwan in 2016 caused a spike in the dynamics of cross-strait relations. The DPP is said to have raised the subject of Taiwanese independence by opposing the 1992 consensus and the One China Policy (Deb, 2023). This caused China to label DPP as a separatist force (Xinhua, 2021). China has slammed the DPP's action and has pointed out that it is colluding with external forces and has become a pawn for anti-China forces (Xinhua, 2022b).

Table 5.4 Total PLA Violations of Taiwan's De-Facto ADIZ

Year	*Sorties*
2018	0
2019	11–20
2020	381–390
2021	972
2022	3101–3119
2023 till November	1652

As a result, China's forceful approach with regard to Taiwan has increased since 2016. China has entered the Taiwanese Air Defense Identification Zone (ADIZ) and has also increased its air and naval operations around the island. According to the information gathered by Taiwan's Ministry of Defense, since 2019, there have been significantly more incursions (Table 5.4).

It can be argued that one of the factors driving China's forceful moves surrounding Taiwan has been the wedge in Sino-US ties. By signing the Taiwan Travels Act in 2018, the US moved to strengthen its relationship with Taiwan and promote official visits (Wees, 2018). Additionally, the US and Taiwan have increased their levels of defense collaboration. Nonetheless, US House Speaker Nancy Pelosi's visit to Taiwan in 2022 marked a seismic shift in US policy. After this event, China carried out one of the most rigorous military drills in the vicinity of Taiwan (Lee & Wu, 2022). Live missiles have been fired during drilling for the first time since 1996. By breaching the middle line that divides the airspace above the Taiwan Strait between China and Taiwan, China has increased its aerial activity. China had only crossed this midpoint line 23 times between September 2020 and May 2022; post-Nancy Pelosi's arrival, the number of crossings increased to 563 (Shattuck, 2023). This amplification illustrates the extent of China's air operations near Taiwan, as does the ADIZ breach. The actions of Chinese naval assistance in Taiwan have also increased. Since then, China's provocative military drills near Taiwan have become routine. China once again carried out significant drills near Taiwan in 2023, coinciding with the visit to the United States of Taiwan's vice president William Lai (Grundy, 2023). This was a major naval exercise simulating the blockade in Taiwan (Pierson & Chien, 2023). Therefore, the dynamics of China's military activities in Taiwan have been aggravated and have become assertive.

Geopolitical Implications of the Taiwan Strait Crisis

One of the most important straits for connecting Far Eastern manufacturing hubs to the rest of the world is the Taiwan Strait. However, as relations across the Taiwan Strait between China and Taiwan have deteriorated in recent years, there has been an increase in militarization of the area. China has recently increased its military operations to thwart initiatives that would promote

Taiwanese independence. As mentioned above, China has increased its military spending to heights that have not been seen before. Additionally, it released a white paper titled "The Taiwan Question," which asserts unequivocally that reunification is the primary objective and that it may be necessary to use force to achieve it (Xinhua, 2022a). This has led to speculation about the geopolitical implications of a "hot" war across the Taiwan Strait and its implications for the overall dynamics of international politics.

As stated throughout, Taiwan is the global epicenter of semiconductor manufacturing. Advanced chips are essential for the operation of contemporary technologically driven economies. Taiwanese chips are essential for the operation of every major industry, including computers, mobile phones, automobiles, and military hardware. The extent to which this technology influences the global economy is unparalleled. As a result, a cross-strait crisis will cause the manufacture of semiconductors to stop, and the globe will experience a shortage of essential items, including mining and agricultural equipment, as well as telecommunications and medical gadgets (Vest et al., 2022). Since Taiwan is the world's primary supplier of semiconductors, any disruption would shock the entire world economy and cause it to enter a recession. As a comparison, the worldwide inflation rate increased rapidly after the outbreak of the Russia–Ukraine War. Yet Taiwan is far more valuable to the global supply chain than either Ukraine or Russia. This is mostly because the modern economy is powered by semiconductors. Consequently, the global manufacturing supply chain will be severely disrupted by any crisis in the Taiwan Strait (Waelbroeck, Rocha & Biswas, 2021). Owing to a shortage of semiconductors, the COVID pandemic caused significant backlogs in large auto and telecommunication orders, which affected the worldwide manufacturing supply chain. Therefore, if semiconductor production is not diversified at the time of such a clash across the Taiwan Strait, a full-blown crisis will be harmful to all the main economic sectors.

Consequently, countries are now connecting semiconductors to national security. According to a US senator, the country's economic and national security is highly vulnerable owing to the semiconductor manufacturing industry (Wei, 2022). This is mostly because of its wide range of applications, including AI, next-generation technologies, and defense. Therefore, any disruptions in supply could undermine a country's national goal if it depends on outside suppliers for the provision of such an essential substance. This makes it evident that Taiwan's semiconductor supply chain is vital to the rest of the world. Given that China is one of Taiwan's largest importers of semiconductors, this also applies to China. The import of semiconductors from Taiwan costs China more than its overall crude imports (Sheng, 2021). This demonstrates the enormous geopolitical relevance Taiwan possesses, even for China, given that Taiwan is the primary supplier of semiconductors for advanced manufacturing and next-generation technology. Despite recent efforts to expand its presence in industry, China still relies principally on Taiwan for semiconductor manufacturing. This explains why China, while having banned a number of Taiwanese

goods including agricultural items following US Speaker Nancy Pelosi's visit to Taiwan, did not extend the boycott to semiconductors (Chiang, 2022).

Therefore, a crisis in the Taiwan Strait would be a major blow to the overall global economy. The world's dependency on Taiwan for advanced semiconductors is expected to grow further in the coming years. This will make nations dependent on Taiwan for semiconductors, which is crucial for their national interests. With the increased levels of US-China competition, the dynamics of international politics are shifting significantly. Nations now want to be self-reliant and independent of others, principally when it comes to the issue of core national interests that semiconductors have now become. This is a leading nation, such as the US, China, and the EU, to push production, supply chains, and innovation in their respective regions. This fundamentally challenges global interdependence, which is a key segment of modern-day globalization. Therefore, the present dynamics of international politics have made nations self-protective by maintaining national interests and security.

Security Outweighing Interdependency—A Critic of Complex Interdependency Theory Regarding Taiwan's Strait Crisis

With the collapse of the Soviet Union, a new era of globalization began, with countries now depending on one another for economic activity. As a result of the interdependence and entanglement of national economies, the global economy as a whole would suffer if one country's economy were to suffer a setback. The concept of complex interdependency, first introduced by Keohane and Nye in their 1970 book *Power and Interdependency: World Politics in Transition*, was furthered by this concept. The core tenet of complex interdependency theory is that the likelihood of military and coercive force decreases as governments' economic ties grow (Nye & Keohane, 1977). In international relations, the liberal school of thought is based on the notion that economic interdependence and interaction lessens the likelihood of war. It is believed that, under conditions of interdependency, when countries rely on one another for economic support, they would prefer to trade rather than invade because this would benefit both parties. Liberals believe that peace is the result of a high degree of interdependency (Poufinas & Pistikou, 2018). However, for the realist school, security and power are the key aspects that would guarantee a nation's survival. In an anarchic world, security for nations are guaranteed by itself, as nations have to enhance their respective capabilities and depend on others for objects that are significant for national power will deter one's security and power, which would be a cause for war (Copeland, 1996).

This notion of economics outweighs that of security, and war between nations is not new. Prior to World War I, the interdependency between nations in Europe was at its highest, and it was argued that it would be the driving force in preventing war. However, the outbreak of the war became a major source of criticism for the overall notion of complex interdependency (Papayoanou, 1996). It has to be argued that nations would always strive for security and

power, which is the key to the anarchic nature of international politics. Even if the two nations are dependent on each other for economic purposes, a step taken by one of the nations that endangers the security of the other would lead the other to instigate actions that could lead to conflict, as upholding security is primary for nations.

In the context of the Taiwan Strait, political dynamics fundamentally revolve around security and national interest. From China's standpoint, the ultimate status of Taiwan is unquestionable and reunification is a matter of the utmost significance. The concept of security has garnered more significance overall in the Chinese political landscape. During the 20th Party Congress in 2022, the Chinese president emphasized security more than economic progress, which he mentioned 91 times during his speech (Bloomberg News, 2022). This is a major shift from previous occasions when economics was given more emphasis than security. This proves that the question of Taiwan is garnering more overall significance in Chinese politics. Taiwan is a key security issue for Beijing, and, as mentioned, the rejuvenation of the Chinese nation cannot be completed without Taiwan's reunification with the mainland. Taiwan has exported semiconductors worth $350 billion to China in 2020 alone (Sheng, 2021). This illustrates the Chinese economy's reliance on the Taiwanese semiconductor supply chain. From the context of complex interdependence, greater economic integration between both nations would shed aside war and acts of coercive force. However, when there is a question regarding Taiwanese independence, China has been clear that it would reside in using force to stop it and unify Taiwan with the mainland.

Recently, there has been an increase in the number of Chinese aggressive and coercive acts around Taiwan. Although China is still very much dependent on Taiwan for semiconductors, it has not hesitated to put forward a show of force around the Taiwan Strait in recent years. Many argue that a declaration of Taiwanese independence would provoke a Chinese military response against Taiwan, disrupting its semiconductor supply chain. Therefore, is semiconductor and trade with Taiwan more significant than allowing Taiwan to be independent? This is clear for China, which has reiterated it on several occasions. Therefore, security always outweighs interdependence, as nations can be dependent on the other for certain goods in matters of one's security, however, there will not be any compromise. For China, Taiwan is a key security and nation interest issue, and being dependent on Taiwan will not be sufficient to prevent a cross-strait war if there are calls for Taiwanese independence. This is well understood by the international community, which is leading nations to shift the semiconductor supply chain in their respective nations. If interdependence was the key to enhancing relations and preventing war, then why would the US and the EU push to move the semiconductor supply chain to their respective zones? This is mainly the result of issues of security and national interests. Semiconductors have become a matter of core security and national interest issues, and nations do not want any disruption in their supply chain, which restricts their power holdings. Therefore, the notion of complex

interdependency in the case of semiconductors does not occur, and it is not sufficient to prevent a cross-strait crisis.

Conclusion

As semiconductors have become the core aspect of modern-day economies, the significance of Taiwan is also increasing. This is fundamentally because of its role as a hub for semiconductor manufacturing. In addition, the country's share in the production of high-end global semiconductors is increasing, spearheaded by the TSMC. This has made nations and the global economy dependent on Taiwan to supply advanced semiconductors. Therefore, any disruption in the semiconductor supply chain will impact the entire global economy.

References

Bloomberg News. 2022, October 18. Xi Mentions of 'Security' Eclipse 'Economy' in Historic Shift. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-10-18/xi-mentions-of-security-eclipse-economy-in-historic-shift

Campbell, C. 2021, October 1. From Phones to Cars and Fridges, This Taiwan Firm Powers the World. But Success Brings Problems. *Time*. https://time.com/6102879/semiconductor-chip-shortage-tsmc/

Chiang, M.-H. 2022, December 3. *China Can't Afford to Ban Taiwan's Semiconductors*. East Asia Forum. https://www.eastasiaforum.org/2022/12/03/china-cant-afford-to-ban-taiwans-semiconductors/

Copeland, D. C. 1996. Economic Interdependence and War: A Theory of Trade Expectations. *International Security*, *20*(4): 5–41. https://doi.org/10.2307/2539041

Crawford, A., Dillard, J., Fouquet, H., & Reynolds, I. 2021, January 25. The World Is Dangerously Dependent on Taiwan for Semiconductors. *Bloomberg.Com*. https://www.bloomberg.com/news/features/2021-01-25/the-world-is-dangerously-dependent-on-taiwan-for-semiconductors

Cronin, R. 2022, August 16. Semiconductors and Taiwan's "Silicon Shield". *Stimson Center*. https://www.stimson.org/2022/semiconductors-and-taiwans-silicon-shield/

Culver, J., & Hass, R. 2021, March 30. *Understanding Beijing's Motives Regarding Taiwan, and America's Role*. Brookings. https://www.brookings.edu/articles/understanding-beijings-motives-regarding-taiwan-and-americas-role/

Dasgupta, S. 2022, August 10. *Race for Semiconductors Influences Taiwan Conflict*. Voice of America. https://www.voanews.com/a/race-for-semiconductors-influences-taiwan-conflict-/6696432.html

Deb, S. 2023. January 30. An Unavoidable Crisis: The Changing Dynamics of Cross-Strait Relations. *Institute for Security and Development Policy*. https://isdp.eu/an-unavoidable-crisis-the-changing-dynamics-of-cross-strait-relations/

Dimerco. 2023, October 10. *Taiwan's Strategic Role in the Global Semiconductor Supply Chain*. Dimerco. https://dimerco.com/taiwans-strategic-role-global-semiconductor-supply-chain/

Ding, M., White, E., Liu, N., & Liu, Q. 2022, September 28. China's Big Fund Corruption Probe Casts Shadow Over Chip Sector. *Financial Times*. https://www.ft.com/content/8358e81b-f4e7-4bad-bc08-19a77035e1b4

Fang, C. T. 2022, September 14. *Apple to Use TSMC's next 3-nm Chip Tech in iPhones, Macs Next Year*. Nikkei Asia. https://asia.nikkei.com/Business/Tech/Semiconductors/Apple-to-use-TSMC-s-next-3-nm-chip-tech-in-iPhones-Macs-next-year

France 24. 2019, January 2. China's Xi Threatens Taiwan with Force but also Seeks Peaceful "Reunification". *France 24*. https://www.france24.com/en/20190102-china-xi-jinping-says-taiwan-reunification-inevitable-military-force

Grundy, T. 2023, August 19. *China Launches Military Drills Around Taiwan as "Stern Warning," after Island's Vice-Pres Visits US*. Hong Kong Free Press HKFP. http://hongkongfp.com/2023/08/19/china-launches-military-drills-around-taiwan-as-stern-warning-after-islands-vice-pres-visits-us/

Gustafson, J. L. 2011. Moore's law. In *Encyclopedia of Parallel Computing*, 1177–1184, edited by D. Padua. Springer US. https://doi.org/10.1007/978-0-387-09766-4_81

Hsu, J. 2017. State Transformation and the Evolution of Economic Nationalism in the East Asian Developmental State: The Taiwanese Semiconductor Industry as Case Study. *Transactions of the Institute of British Geographers*, *42*(2): 166–178. https://www.jstor.org/stable/45147080

Lee, L. C. 2024, June 6. China's Big Fund 3.0: Xi's Boldest Gamble Yet for Chip Supremacy the Third Phase of Beijing's Semiconductor Policy Aims to Learn from Past Mistakes. As Stakes Rise, Can Xi Jinping Secure China's Tech Future and Cement his Political-Economic Legacy? *The Diplomat*. https://thediplomat.com/2024/06/chinas-big-fund-3-0-xis-boldest-gamble-yet-for-chip-supremacy/

Lee, Y., & Wu, S. 2022, August 5. Furious China Fires Missiles Near Taiwan in Drills after Pelosi Visit. *Reuters*. https://www.reuters.com/world/asia-pacific/suspected-drones-over-taiwan-cyber-attacks-after-pelosi-visit-2022-08-04/

Liu, L. 2019, October 30. China's 'Big Fund' Phase II Aims at IC Self-Sufficiency. *EE Times*. https://www.eetimes.com/chinas-big-fund-phase-ii-aims-at-ic-self-sufficiency/

Liu, Y. 2020, January 1. *From Deng to Xi, a Look Back at 40 Years of Reunification Efforts across Taiwan Strait*. CGTN. https://news.cgtn.com/news/2020-01-01/40-years-on-National-reunification-always-deep-desire-of-all-Chinese-MTmg8tQCdi/index.html

Ma, J. 2023, March 30. China's 'Big Fund II' Makes Intensive Investments, as Country Aims to Overcome US Chip Ban—Global Times. *Global Times*. https://www.globaltimes.cn/page/202303/1288294.shtml

Matta, M. 2023, September 8. Council Post: The Future of Renewable Energy Is Built on Semiconductors. *Forbes*. https://www.forbes.com/councils/forbesbusinessdevelopmentcouncil/2023/09/08/the-future-of-renewable-energy-is-built-on-semiconductors/

Mok, C. 2023, August 23. The Party Rules: China's New Central Science and Technology Commission. *The Diplomat*. https://thediplomat.com/2023/08/the-party-rules-chinas-new-central-science-and-technology-commission/

Nye, J. S., & Keohane, R. O. 1977. *Power and Interdependence: World Politics in Transition*. Little, Brown, and Company.

Palmer, A. W. 2023, July 12. 'An Act of War': Inside America's Silicon Blockade against China. *The New York Times*. https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html

Papayoanou, P. A. 1996. Interdependence, Institutions, and the Balance of Power: Britain, Germany, and World War I. *International Security*, *20*(4): 42–76. https://muse.jhu.edu/pub/6/article/447423

Pierson, D., & Chien, A. C. 2023, September 14. China Conducts Major Military Exercises in Western Pacific. *The New York Times*. https://www.nytimes.com/2023/09/14/world/asia/china-ships-taiwan-japan.html

Poufinas, T., & Pistikou, V. 2018. A Financial Analysis Approach on the Promotion of Peace through Economic Interdependence. *Theoretical Economics Letters*, *8*(15): Article 15. https://doi.org/10.4236/tel.2018.815222

Schumacher, A. 2024. *China's Mature Semiconductor Overcapacity: Does It Exist and Does It Matter?* https://www.csis.org/analysis/chinas-mature-semiconductor-overcapacity-does-it-exist-and-does-it-matter

Shattuck, T. 2023, September 20. *One Year Later: How Has China's Military Pressure on Taiwan Changed Since Nancy Pelosi's Visit?* Global Taiwan Institute. https://globaltaiwan.org/2023/09/one-year-later-how-has-chinas-military-pressure-on-taiwan-changed-since-nancy-pelosis-visit/

Sheng, W. 2021, April 29. *China Spends More Importing Semiconductors than Oil · TechNode*. TechNode. http://technode.com/2021/04/29/china-spends-more-importing-semiconductors-than-oil/

Taiwan Today, M. of F. A. 2010, June 18. *Veteran Tells Story of Taiwan's Semiconductor Industry* [Website]. Taiwan: Taiwan Today; Ministry of Foreign Affairs, Republic of China. https://taiwantoday.tw/news.php?unit=6&post=9508

Tang, F., & Ji, S. 2023, February 8. *Starved of Chips, China Faces 'Unprecedented' Pressure to Become No 1 Economy*. South China Morning Post. https://www.scmp.com/economy/china-economy/article/3209385/tech-war-starved-semiconductors-chinas-bid-topple-us-no-1-economy-faces-unprecedented-pressure

US Department of State. (n.d.). *Milestones: 1953–1960—Office of the Historian*. Office of Historian. Retrieved December 11, 2023, from https://history.state.gov/milestones/1953-1960/taiwan-strait-crises

Vest, C., Kratz, A., & Goujon, R. 2022, December 14. The Global Economic Disruptions from a Taiwan Conflict. *Rhodium Group*. https://rhg.com/research/taiwan-economic-disruptions/

Waelbroeck, Rocha E., & Biswas, R. 2021, November 8. *Sharing Insights Elevates Their Impact*. S&P Global. https://www.spglobal.com/marketintelligence/en/mi/research-analysis/taiwan-crisis-scenario-disrupt-global-supply-chain.html

Wees, G. van der. 2018, March 19. The Taiwan Travel Act in Context. *The Diplomat*. https://thediplomat.com/2018/03/the-taiwan-travel-act-in-context/

Wei, C. 2022, April 21. Are Semiconductors a National Security Issue? *The Diplomat*. https://thediplomat.com/2022/04/are-semiconductors-a-national-security-issue/

Wu, D. 2022, December 29. TSMC Starts Next-Gen Mass Production as World Fights Over Chips. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-12-29/tsmc-mass-produces-next-gen-chips-to-safeguard-global-lead

Xinhua. 2021, July 28. Separatist Forces Advocating "Taiwan Independence" Doomed to Fail: Spokesperson-Xinhua | English.news.cn. *Xinhua Net*. http://www.xinhuanet.com/english/2021-07/28/c_1310092044.htm

Xinhua. 2022a, August. Full Text: The Taiwan Question and China's Reunification in the New Era-Xinhua. *Xinhua Net*. https://english.news.cn/20220810/df9d3b8702154b34bbf1d451b99bf64a/c.html

Xinhua. 2022b, March 1. Mainland Slams DPP Seeking "Taiwan Independence" by Banking on External Forces-Xinhua. *Xinhua Net*. https://english.news.cn/20220301/3255140fd7414253b194eba327ed7e6c/c.html

Yahoo Finance. 2023, September 25. TSMC's 2nm Chip Production Possibly Delayed Until 2026 Amid Semiconductor Demand Slowdown. *Yahoo Finance*. https://finance.yahoo.com/news/tsmcs-2nm-chip-production-possibly-013235088.html

6 Assessing Technology as a Key Driver in Geopolitics

The Case of India

Achal Malhotra

Introduction

A strong leadership, political stability and political will, vision, a robust economy, a strong science and technology base and powerful military capability are amongst the important elements which determine the stature of a given nation in the global hierarchy. In this context, technological innovations and their skillful application are arguably extremely important enabling factors in achieving economic and military parity or superiority on the global arena. This is as true in our contemporary world as it was in both the distant and ancient past and in relatively recent medieval times.

Historically, technological inventions have played a crucial role in the evolution of human civilization from time immemorial. Several of these inventions have been truly game-changers. For centuries, these inventions have helped to make the lives of human beings easier, better organized and, to some extent, have helped them to gain superiority over surrounding environments, in addition to contributing immensely to the material progress of human civilization. For instance, millions of years ago, the invention of basic tools was instrumental in gaining advantage for the hunters over animals, which were their major source of food. The invention of fire was useful in more than one sense: physical comfort (warmth in cold climates), weapons, and, more importantly, improved nutrients through the provision of cooked food and the enlarging of the human brain which led, in turn, to further inventions. The development of agriculture led to revolutionary changes in the way the human beings lived and behaved: from wanderers to settlers, the formation of societies and social classes. Similarly, the invention of the wheel was first of assistance in the area of agriculture and, later, in the wider sphere of transportation.

The technological inventions of relatively recent centuries have, in many cases, turned out to be both constructive and destructive. More importantly, the possession of such technologies has helped individual nations, or groups of nations, gain geopolitical superiority/advantage over other nations. The military advantage of the "The Gun Powder Empires" over their rivals has been widely recorded in global history. The mastery of navigation and ship building technology helped European powers gain maritime advantage and this, in turn,

DOI: 10.4324/9781003633204-7

acted as an enabling factor in the colonization of alien lands. The first ever use of an atom bomb as a weapon of war by the Allied Forces on Japanese territory (Hiroshima and Nagasaki on 6 and 11 August 1945, respectively) ended World War II, albeit at and enormous cost to civilian lives and a dreadful impact on human beings and the environment which continued for many decades. There are countless such examples. This essay seeks to focus on the strengths of India's technological prowess in selected areas and the consequential impact on its position in regional and global geopolitics.

The Case of India

India is one of the most ancient civilizations in the world; it was also an advanced civilization by the standards and yardsticks of those times. There is enough evidence to establish that a number of the landmark discoveries in areas such as mathematics, astronomy, medicine, architecture were first made in ancient and medieval India, which in turn laid the foundations of modern science and technology. For instance, the archaeological discoveries show that fairly advanced systems of agriculture, sewage and drainage systems existed as early as Indus Valley civilization, which dates back to earlier than 5000BC. In the field of mathematics, the concept of the zero (0) was first defined by the 7th-century mathematician Brahamagupta. Similarly, the "decimal system" was developed by the noted mathematician and astronomer Aryabhatta (5th century AD), who was also the first to explain the true causes of solar and lunar eclipses, that the shape of the Earth was not flat but cylindrical, that the Sun was stationary, and that it was the Earth which revolved around the Sun. *Aryabhatta*). Varahamira, another famous astronomer of the time, discovered that the Moon rotates around the stationary Earth (Varahamira's book *Brihat Samhita*). Needless to say, the list is only illustrative. However, the pathbreaking achievements of the past were somewhat over-shadowed by the colonization of India by the British from the 19th century onwards. Yet these cumulative achievements of the past in science, technology and medicine helped India carve a special place for itself on the global horizon in those times.

The Reflection of Independent India's Strengths in Science and Technology on its Global Stature

India's quest for an advanced country in terms of a developed industrial sector and high levels of science and technology began from the beginning as soon as India attained independence from the British rule on August 15, 1947. The colonizers can be credited with unifying the Indian intelligentsia through the English language and the country through the introduction of railways. On the whole, however, India emerged as an impoverished country in 1947 due to its ruthless exploitation by the colonizers in their own national interests. The Indian leadership of independent India realized the importance and role of science and technology in addressing the problems of economic and social

backwardness in India of those years. In this context, the role of independent India's first Prime Minister Pandit Jawaharlal Nehru stands apart. He was a great visionary, who firmly believed that the consequences of science were more important than science itself. Nehru had a strong faith in science and its application in resolving the enormous problems arising out of primitive agriculture, a poor industrial base, poverty etc. confronting the newly independent India. Nehru's vision of the role of science in national reconstruction was reflected in the Scientific Policy Resolution adopted by the Indian Parliament on March 4, 1958. This stated: "It is an inherent obligation of a great country like India with its traditions of scholarship and original thinking and its great cultural heritage, to participate fully in the march of science which is probably mankind's greatest enterprise today."

While talking about science and its social consequences, Nehru often emphasized the importance of spreading "scientific temper" in the country—a concept he articulated in his book *The Discovery of India*, published in 1946. In short, Nehru was of the opinion that it was essential to first develop a scientific temper or scientific approach or scientific method so that the full benefits from the development of science and technology could be derived. Nehru's concept of a scientific temper was incorporated into the Fundamental Duties of every citizen of India in the Constitution of India and reads as follows: "It shall be the duty of every citizen of India to develop a scientific temper, humanism and the spirit of enquiry and reform."[1] The initiatives unveiled in the immediate post-independence period by the leaders of the newly independent India were augmented then and subsequently by illustrious scientists/administrators, such as Homi Jehangir Bhabha,[2] Dr Vikram Sarabhai,[3] A.P.J. Abdul Kalam,[4] Sam Petroda,[5] M.S, Swaminathan[6] (to name a few), were instrumental in laying out the strong foundations of science and technology and its applications, including the establishment of such premier institutions as the Bhabha Atomic Research Centre (BARC) in the field of nuclear science, and the Indian Space Research Organization (ISRO) in the area of space science, in addition to the Indian Institute of Science, and the Indian Institute of Technology (all within a decade or so of independence) and, later, the Centre For Development of Telematics (C DOT)[7] in the field of telecommunications.

Evolution of Technology in Post-independence India in Selected Areas

Over the course of its post-independence history, India, backed by science and technology, has registered considerable progress in several fields, while there are also areas in which much remains to be done. In sectors such as Nuclear Technology, Space Technology and Information and Communication Technology, India has emerged as a competitive global player, whereas commendable accomplishments have been made in Agriculture. India is now engaged in its efforts to catch up with rest of the world in the manufacturing of semiconductors, in the field of artificial intelligence, cyber science and advanced cutting-edge defence technologies. In what follows, I will focus on

the accomplishments in the following areas which have put India on the global map and enhanced its hard and soft power.

Agriculture

When India attained independence from the British rule in 1947, its agriculture sector was in a poor state. The situation was exacerbated by the fact that a significant chunk of the fertile land went to the share of Pakistan as a result of India's partition in 1947. The productivity of wheat, rice, maize and total food-grains in Pakistan was 40% higher than in India. Food shortages led to a situation in which India had to depend on US Aid for foodstuffs. The founding leaders of India realized the importance of food security. The then Prime Minister Jawaharlal Nehru is often cited as having remarked that: "Everything else can wait but not agriculture."

The situation once described by the noted agricultural scientist as "from ship to mouth" has undergone tremendous change. Thanks to a series of revolutions, including the Green Revolution, White Revolution and so on, India has now not only attained food security for itself but also finds itself in a position to export food grains. India is now the world's second-largest producer of wheat. In 2021, India exported a record 7 million metric tons (MT) of wheat which was valued at $2.05 bn. India's share in the global trade of rice is estimated to be as high as 45%.

During the Covid pandemic and beyond, India supplied several thousand MT of food as humanitarian assistance in the form of wheat, rice, pulse, lentils to a large number of countries all over the world, including Afghanistan, Comoros, Djibouti, Eretria, Lebanon, Madagascar, Malawi, the Maldives, Myanmar, Siera Leone, Sudan, South Sudan, Syria, Zambia, Zimbabwe, to strengthen their food security. It is worth noting that the food aid was in addition to the ambitious food-support programme which the Government of India had introduced for its own 841 million poor and needy people. The commitment to Afghanistan alone was 50,000 MT. It should be noted here that both Russia and Ukraine account for over 30% of global wheat grains supplies. Therefore, the outbreak of the military conflict between Russia and Ukraine in February 2022 resulted in serious disruptions in food supply chains and created food insecurity in many countries. Against this backdrop of volatility in global food markets, India's role as an alternate source of supplies assumed importance.

On May 13, 2022, the Government of India was required to announce restrictions on wheat exports, primarily to focus on "meeting domestic demands while protecting farmers' incomes."[8] Nevertheless, India continued to remain "committed to the genuine needs of neighbouring countries and food deficient nations through Government-to-Government mechanisms and also to fulfil supply commitments already made."[9] Thus, over 1.8 MT of wheat were shipped to countries such as Afghanistan, Bangladesh, Bhutan, Israel, Indonesia, Malaysia, Nepal, and many other countries. Later, in July 2023, India's decision to regulate the export of non-basmati rice to address domestic demand created a situation

of serious concern in global markets and amongst the major players, including the USA, Japan, Australia, Brazil etc.[10] The issue was considered serious enough for them to raise it at a meeting of the World Trade Organization (WTO). A government of India's Geneva-based official was quoted as having said that the USA, Japan and other countries had "expressed concern about the impact of India's export ban on the global food market highlighting its significance as the world's largest rice exporter accounting for over 40% of global exports." The world leader, USA, was reported to have urged India to lift the ban.

Once again, despite the ban, which India describes as a temporary regulatory measure rather than restrictions,[11] the country continues to supply wheat and rice to food-deficient, vulnerable countries, particularly its neighbours and strategic partners, such as Nepal, Bhutan, Sri Lanka Malaysia, Indonesia, Vietnam, and Iran, through government mechanisms.

In summary, it is abundantly clear from the above narration that the application of agro-science and technology-backed revolutions have changed the face of agriculture in India since 1947, when the country attained independence and in a period when its agriculture was in a poor state. The net outcome of these revolutions is that India has ensured food security for its population of nearly 1.4 billion. More importantly, the importance of India as an important supplier in the global food supply chains is now well established, and this has been possible thanks to the mastering and application of appropriate technology in agriculture. The country has often used its strength as a soft power to generate goodwill amongst food-deficient countries, particularly in the global south, for whom India is aspiring to be a leader.

Nuclear Technology

Over the years, India has mastered complete nuclear cycle capabilities. It thus has the technology for both civilian and military purposes. Accordingly, India has added nuclear power to its energy mix, using nuclear technology in other civilian areas such as nuclear medicine and the desalination of water. At the same time, India is also in possession of nuclear weapons. At the moment, the share of the nuclear power for civilian purposes in the total installed capacity remains low, at around 2%. However, India's status as a de facto nuclear weapon state, despite being outside the Nuclear Non-proliferation Treaty (NPT), is well-established. This, in turn, has had a significant impact on geostrategic deterrence in the region, where India is surrounded by two adversary nuclear powers: China in the North and Pakistan in the West. The journey on the path for the development of nuclear capabilities, for both civilian purposes and nuclear weapons capacities, has been incremental but also long and arduous.

The Beginning: Preference for Nuclear Power Exclusively for Civilian Purposes

India's quest for the development of nuclear power as an important component of its energy mix began around the time India attained independence in

1947. The founder-leaders of the independent India realized the importance of nuclear power as an important contributor in the development of industry and also to meet the civilian needs, which were bound to grow with the passage of time.[12]

Nuclear Programme: Personalities, Legislations/ Institutional Mechanisms

Personalities

India's first Prime Minister Jawaharlal Nehru and the eminent scientist Dr Homi Bhabha are considered to be the architects of India's nuclear programme, which was originally meant for civilian applications, but gradually acquired military dimensions. Both Nehru and Bhabha were adamant about protecting India's atomic sovereignty from international efforts to control nuclear technology. However, prima facie, the two appeared to differ from each other on the issue of making a nuclear bomb by India. On one occasion, in 1951, B.K. Nehru, PM Jawaharlal Nehru's cousin and the Indian Ambassador to the USA, asked Bhabha why was he not planning to construct a bomb. The scientist, in an apparent reference to PM Nehru, replied: "the old man won't let me," adding further that "He (Nehru) has approved of my plans for atomic energy but said under no condition was I to manufacture a weapon," Nehru was amongst the prominent leaders of India's freedom struggle and was repeatedly elected as the prime minister of independent India from 1947 onwards.[13] He remained so until May 1964, when he died in office of a cardiac arrest. He was an internationalist, an advocate of promoting science and technology, and the founding leader of the Non-Aligned Movement (NAM). In all public statements, he advocated nuclear disarmament and assured people that India's nuclear programme will always be for peaceful applications of nuclear technology.

M.K. Rasgotra, India's former foreign secretary, has revealed, in his book *A Life in Diplomacy*, that United States' President John F Kennedy made an extraordinary gesture towards India by offering help them conduct a nuclear test.[14] He made this offer in a hand-written letter; this was accompanied by a technical note from the chairman of the US Atomic Energy Commission in which he set out the assistance his administration would provide to Indian nuclear scientists to detonate an American device from the top of a tower in the Rajasthan desert. The reason for the offer was that the American intelligence agencies had learnt that China's nuclear programme was progressing towards a scheduled weapon detonation in 1963.[15] Kennedy, who was an admirer of India's democracy and held its leader Jawaharlal Nehru in very high esteem, felt that democratic India, rather than communist China, should be the first Asian country to conduct a nuclear test. Nehru shared the offer with only two persons: G Parthasarathy[16] and Dr Homi Bhabha. After some consideration, the offer was politely declined.

Dr Homi Bhabha was a renowned physicist. He left India in 1927 to study Engineering at Cambridge University but ultimately obtained a doctorate in

Physics in 1934. He had the opportunity to move in the same circles as Frederic-Joliot Curie and the other atomic physicists of the pre-World War II era. In 1939, Bhabha returned to India where he found himself stranded due to the outbreak of the war. He opted for the position of Reader in Theoretical Physics at the Indian Institute of Science in Bangalore (now Bengaluru) where he was promoted in 1941 to Professor of Cosmic Rays. Bhabha was not averse to the idea of making a nuclear bomb. In his book *Homi J Bhabha – A Life*, Bhakhtiar K. Dadabhoy (Rupa Publications, 2023) says that, despite Nehru's rhetoric about nuclear disarmament, Bhabha knew that a time would come when a bomb will have to be made and continued to quietly prepare for it.[17]

Legislative Acts and Institutional Framework

The first steps towards the development of nuclear energy in India were taken as early as 1944, even before the formal attainment of full independence in 1947. On March 12, 1944, Dr Homi Bhabha wrote to Sir Dorabjee Tata Trust about the intention to start nuclear research in India; this led to the inauguration of the Tata Institute of Fundamental Research in Mumbai on December 19, 1945. As a first legislative step, the Indian Parliament adopted the Atomic Energy Act In 1948; this provided the basic framework for the regulation of the use of nuclear energy in India. The objective of this Act was to encourage research on nuclear energy and also increase government control in this field. Under the Act, the Atomic Energy Commission (AEC) was constituted in 1948. This body was entrusted with the survey of minerals such as uranium and thorium, conduct of research and training of scientists in nuclear energy. Uranium exploration and mining required for the nuclear power programme were among the initial activities that were undertaken.

In August 1954, the Department of Atomic Energy (DAE) of the Government of India (GOI) was established. This body is responsible for the execution of policies laid down by the AEC. It is engaged in research, technology development and commercial operations in the areas of nuclear energy, related advanced technologies and supports basic research in nuclear science and engineering. Realizing the importance of developing a strong research and development base for the nuclear power programme, a research and development centre, Atomic Energy Establishment, Trombay (AEET), was inaugurated on January 20, 1957. This was renamed the Bhabha Atomic Research Centre (BARC) in January 1967 following Bhabha's demise. India's nuclear power plan consists of three stages: Stage 1 employs Pressurized Heavy-Water Reactors (PHWR) fuelled by natural uranium to generate electricity and produce plutonium as a by-product; Stage 2 plans to use fast breeder reactors burning the plutonium to breed U-233 from thorium; Finally, Stage 3 proposes to develop this and produce a surplus of fissile material. It may be added that India is deficient in natural uranium reserves, but thorium is available in abundance.

India's Nuclear Weapons Program and the International Non-Proliferation of Nuclear Weapons Regime

It is more or less clear that India under PM Nehru remained committed to the development of nuclear power for peaceful purposes rather than for nuclear weapons, while advocating comprehensive global disarmament. However, the decision to develop a full nuclear cycle gave India the technical capability to pursue nuclear weapons. Nehru passed away on May 27, 1964. By that year, there were already five nuclear powers in the world: three of these, the United States, the Soviet Union, and the United Kingdom, had obtained nuclear capability during or shortly after World War II. France exploded its first nuclear bomb in 1960, and the People's Republic of China joined the club in 1964. According to the Office of the Historian of the US State Department, by the mid-1960s "There were many other countries that had not yet tested weapons, but which were technologically advanced enough that should they decide to build them, it was likely that they could do so before long".[18] It further added:

> Given the excessive costs involved in the development and deployment of new and more technologically advanced nuclear weapons, both powers (USA and Soviet Union) had an interest in negotiating agreements that would help to slow the pace of the arms race and limit competition in strategic weapons development.[19]

The Treaty on the Non-Proliferation of Nuclear Weapons

The resolution moved by Ireland and adopted by consensus in the UN General Assembly in 1961 laid the basis for the negotiation of an international agreement on non-proliferation; the resolution essentially envisaged that countries already having nuclear weapons would "undertake to refrain from relinquishing control" of them to others and would refrain "from transmitting information for their manufacture to States not possessing" them. Under this agreement, countries without nuclear weapons would agree not to receive or manufacture them. After protracted negotiations which began in 1965 in the UN Conference on Disarmament, finally the Treaty on the Non-Proliferation of Nuclear Weapons, commonly known as the Non-Proliferation Treaty or NPT, was concluded and opened for signatures on July 1, 1968 and entered into force on March 5, 1970. One of the outcomes of the NPT was that the five States which had manufactured and exploded a nuclear weapon prior to January 1, 1967 (the USA, Russia, the UK, France and China) acquired the Status of Nuclear-Weapon States, whereas all other countries were to be treated as Non -Nuclear Weapons States. Incidentally, these five countries are also the five Permanent Members of the UN Security Council. The remaining countries in the rest of the world who opted to be a party to the Treaty automatically acquired the permanent status of non-nuclear weapon States.

Based on the provisions of the Treaty, one can surmise that the Treaty was a bargain between the Nuclear Weapons states and Non-Nuclear Weapons States in which those countries aspiring to acquire nuclear weapons (such as India) were excluded conveniently.[20] The Nuclear Weapons States agreed *not* to assist in any manner any non-nuclear weapon State in acquiring nuclear weapons technology/weapons, but agreed to assist non-nuclear weapons States in the development of nuclear technology for peaceful purposes. In return, the non-Nuclear States were required to conclude appropriate safeguards agreements with the International Atomic Energy Agency (IAEA) so that they could keep a track of their nuclear programme. The Nuclear-weapon States also agreed to "pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament, and on a treaty on general and complete disarmament under strict and effective international control."[21]

In the years preceding the start of negotiation on NPT, the internal debate in India did not lead to any explicit consensus on the development of nuclear technology for military purposes. While the scientists and the security establishment were in favour, the political leadership was not inclined to do so and wanted to follow a policy of insisting on comprehensive disarmament. India participated actively in the NPT negotiations as a country without nuclear weapons.[22] However, the Treaty in the offing was discriminatory from its own perspective as it gave select certain rights and status to five nuclear-weapon States, which were denied to non-nuclear weapon states, including India. India wanted to retain the option to produce its own nuclear weapons, and its neighbour China (with whom India had fought and lost a war in 1962) was already in possession of a nuclear bomb. Pakistan, another adversary of India, refused to join because India would not. Israel, which the United States had tried to restrain from acquiring nuclear weapons in separate negotiations during the 1960s, also refused to join.

India's First Nuclear Explosion: International Reaction

Lal Bahadur Shastri succeeded Nehru as India's prime minister. This year, 1964, was also the year when China exploded a nuclear device. PM Shastri authorized theoretical work on the Subterranean Nuclear Explosion for Peaceful Purposes (SNEPP) project in November 1964. The political decision to conduct a "Peaceful Nuclear Explosion" on May 18, 1974 was taken by then Prime Minister Mrs Indira Gandhi. The location of the nuclear test, code-named "Smiling Buddha", was Pokhran in the deserts of Rajasthan.[23] Accordingly, the test is also described as the Pokhran1 Test.

This nuclear test was the result of the "verbal authorization" by PM Indira Gandhi on September 7, 1972 to BARC scientists to manufacture the nuclear device they had designed and to prepare it for a test. The team was led by the director of BARC, Dr Raja Ramana and the entire operation was kept top secret. India's 1974 peaceful nuclear explosion (PNE) had expected condemnation,

particularly from the USA and Canada; it was regarded as a serious threat to NPT and, to a great extent, it also led to the formation of Nuclear Suppliers Group (NSG). India, however, continued to maintain that the PNE was a part of India's pursuits for peaceful uses of nuclear energy. The weaponization programme was authorized by PM Rajiv Gandhi, who succeeded Indira Gandhi following her assassination in October 1984. The decision was taken in the backdrop of the Brasstacks Crisis, which was a nuclear scare between India and Pakistan.[24] The massive military exercises (November 1986 to January 1987) conducted by the military also drew a strong reaction from Pakistan, which began to threaten India with a nuclear attack.

Much has been written about PM P.V. Narasimha Rao's decision to put on hold a nuclear explosion under American pressure. In an interview in 2004, the eminent journalist Shekhar Gupta confronted him with a direct question as to whether there had been pressure from the Americans on India not to conduct another nuclear test. The key line in his response was: "This secret will perish with me."[25] India waited for a period of 24 years since the first PNE before, under the leadership of PM Atal Bihari Vajpayee, it conducted two further nuclear explosions, on May 11 and 13, 1998. With these nuclear tests India formally became a nuclear weapon state, albeit one outside the NPT. India's nuclear tests were followed within a month by similar tests by Pakistan. The adverse reaction from the West was along the expected lines, with sanctions being imposed on both India and Pakistan.

India's Nuclear Doctrine

On January 4, 2003, the Cabinet Committee on Security revealed the following elements of India's nuclear doctrine:

i Building and maintaining a credible minimum deterrent;
ii A posture of "No First Use" i.e., nuclear weapons will only be used in retaliation against a nuclear attack on Indian territory or on Indian forces anywhere;
iii Nuclear retaliation to a first strike will be massive and designed to inflict unacceptable damage.
iv Nuclear retaliatory attacks can only be authorized by the civilian political leadership through the Nuclear Command Authority.
v Non-use of nuclear weapons against non-nuclear weapon states. However, in the event of a major attack against India, or Indian forces anywhere, by biological or chemical weapons, India will retain the option of retaliating with nuclear weapons;
vi A continuance of strict controls on export of nuclear and missile related materials and technologies, participation in the Fissile Material Cutoff Treaty negotiations, and continued observance of the moratorium on nuclear tests.
vii Continued commitment to the goal of a nuclear weapon free world, through global, verifiable and non-discriminatory nuclear disarmament."

In its 2014 Election Manifesto, the Bhartiya Janata Party (BJP) announced its intention to "revise and update India's nuclear doctrine."[26] However in the 10 years of BJP-led government (2014–2024), there has not been any public discourse on this topic, except on one occasion when an indication was given that India may review one of the core elements of the doctrine, namely the "No First Use" of nuclear weapons. On 16 August 2019, India's Defence Minister Raj Nath Singh said that "It is true that until now, India has strictly adhered to the 'No First Use' policy. But what happens in the future depends on the circumstances."[27] This statement came against the backdrop of mounting tensions between India and Pakistan over India's decision to abrogate Article 370 of its Constitution and end the special status of Kashmir, and also repeated threats, from time to time, around the use of nuclear weapons by Pakistan against India. And, therefore, the statement could more accurately be seen as a message to Pakistan.

Change of Heart in the USA towards India as a Nuclear Weapons State

For decades, the Americans took a hard line on India's nuclear weapons program and status. However, a significant change became visible in the US policy during the then PM Dr Manmohan Singh's visit to USA in July 2005. President Bush not only acknowledged India's impeccable record in non-proliferation of nuclear weapons but also admitted that "as a responsible state with advanced nuclear technology, India should acquire the same benefits and advantages as other such states". He went on to assure the country that he would work to achieve full civil nuclear energy cooperation with India.[28] President Bush said he would also seek agreement from Congress to adjust US laws and policies, and that the United States would work with friends and allies to adjust international regimes to enable full civil nuclear energy cooperation and trade with India.

What followed this historic moment is itself history. India and USA concluded a civil nuclear cooperation agreement in 2008, which was followed by a similar agreement between India and France; India separated its civilian nuclear reactors from the military and placed them under the IAEA safeguards, the Nuclear Suppliers Group (NSG) granted a waiver for its members to enter into nuclear trade with India. Interestingly, all of the major players (the USA, Russia, France, Germany) supported India's case for an NSG waiver. What brought about the change of heart? It appears that the global powers could no more ignore India, as it was now the largest democracy and a country in possession of nuclear weapons, a country which has one-sixth of world population, a country which refused to sign the NPT on the grounds of principles but followed the spirit of the Treaty building up a strong reputation in matters of non-proliferation and global nuclear disarmament and, finally, a country whose economy was growing at impressive rates and which offered enormous opportunities for trade and investments. Today, India is in a unique position; it is the only country outside the NPT which is being engaged by the

global powers for nuclear commerce and cooperation. And this has been possible thanks, inter alia, to India's advancements in nuclear weapons programme and its responsible conduct in matters of non-proliferation.

Space Technology/Information and Communication Technology: Areas of Strength

There are at least two areas where India is at par with developed countries and has a definite competitive edge over a large number of countries; these are: Space and Information and Communication Technology.

India's Space Achievements

In 1962, then India's first Prime Minister, Jawaharlal Nehru, enlisted physicist Vikram Sarabhai to set up the Indian National Committee for Space Research (INCOSPAR). Later, INCOSPAR was superseded by ISRO in 1969 as India's national Space Agency. Over the years, ISRO has steadily built advanced launching and exploration capacities and capabilities, placing it on the world map of space technology and industry. Since the launch of its first satellite *Aryabhata* (designed and fabricated in India) in 1975 India's space programme has travelled a long way.[29] Between 1975 and 2021, ISRO had launched a total of 129 satellites of Indian Origin and 342 foreign satellites belonging to 36 countries, of which nearly 39 satellites are commercial satellites and the rest nano-satellites. There were 53 operational satellites in space, providing various identified services to the nation. At the time, 21 of these were communication satellites, 8 were navigation satellites, 21 were Earth observation satellites and 3 were science satellites.

In July 2023, ISRO undertook a successful mission, Chandrayan 3, the third in the series of lunar exploration missions.[30] With this launch, India became the fourth country to land a spacecraft on the Moon and, more importantly, created history by becoming the first to land in the lunar South Pole region. India is now known across the world for its credible and cost-effective satellite launch missions.[31] According to India's Minister for Atomic Energy and Space, India is now emerging as a hub for the small satellite launch market, which is estimated to reach $38 billion by 2027. The number of foreign satellites launched by India is increasing rapidly. The list of countries which have launched satellites from India includes mostly advanced countries, such as USA, Germany and Singapore.

Information and Communication Technology (ICT)

India's quest for excellence in information and communication technology (ICT) began in real earnest in 1984 when the Centre for Development of Telematics (C-DOT) was established in 1984. It is credited with ushering in a telecommunication revolution, particularly in the rural parts of the country.

In the period since then, India has carved out a niche for itself on the international ICT arena. Both the State and the country's private sector have contributed to the phenomenal growth in this sector. India has done particularly well in creating a large pool of skilled IT professionals, in software development and Business Processing Outsourcing (BPO). The world's corporations have leveraged skilled human resources and established 1500 Global Capability Centres (GCCs) in India, representing 45% of the total number of global GCCs. These centres are currently providing some 5 million jobs in India. A substantial part of India's services exports comes from the IT and BPO. In short, India is now recognized as the world's IT hub and has the potential to emerge as the world's office.[32]

Conclusions

At the very beginning of India's post-independence period, the country's leadership had recognized the importance of science and technology and its skilful application in achieving all-round socio-economic development and it had initiated measures in that direction. Over the years, India's advances in agricultural technology have helped it to ensure food security for its 1.4 billion people and is also emerging as an important player in global food supply chains. The indigenously developed nuclear technology has ensured that India is now a nuclear weapons state, a status which serves as a deterrent for the adversaries in the region. India's impeccable record in the area of non-proliferation despite being positioned outside the NPT is one of the reasons for its international reputation as a responsible nuclear weapons country. India's laudable achievements in space and ICT have added to the country's heft on the global arena. It understands the importance of keeping pace with the rest of the world in critical and emerging technologies in order to sustain its role as a global player.

Notes

1 Government of India (1976) "Fundamental Duties of every Indian Citizen vide Part IV-A, Article 51-A(h)," part of 42nd Amendment to the Constitution of India. New Delhi: Government Printer.
2 Dr. Homi Jehangir Bhabha is the pioneer of the Nuclear Program in India. As early as 1945, he established the Tata Institute of Fundamental Research (TIFR), now deemed a university. In 1954, he established the Atomic Energy Establishment, Trombay (AEET) for the multidisciplinary research program essential for the ambitious nuclear program of India. After the sad demise of Bhabha in 1966, AEET was renamed the Bhabha Atomic Research Centre (BARC). Bhabha also established the Bhabha Training Centre to cater to the manpower needs of the expanding atomic energy research and development program.
3 Dr Vikram Sarabhai is nicknamed the father of India's space programme.
4 Dr APJ Abdul Kalam, a renowned scientist and administrator, often referred to as Missile man, and also as the "Father of Indian Technology" for his contribution to space and missile technology programmes in India. He also served as India's president (July 2002–July 2007).

5 Satyanarayan Gangaram Petroda, mostly known as Sam Petroda was a telecommunication engineer by profession who was the key person in assisting former Prime Minister Rajiv Gandhi to revolutionize information and communication technology in India.
6 A renowned agriculture scientist who introduced several science-backed measures to revolutionize agriculture.
7 C-DOT, the Centre for Development of Technology, set up in 1984, was hailed as the progenitor of the indigenous Telecom Revolution in India.
8 Ministry of Commerce &Industry, Press Release, June 11, 2022.
9 Press Release, Ministry of Consumer Affairs, Food and Public Distribution, Government of India, released by Press Information Bureau, June 25, 2022.
10 Ministry of Commerce & Industry, Government of India dated June 11, 2023.
11 "Export Ban on Rice Is Regulation rather than Restriction", *Hindu*, September 28, 2023. https://www.thehindu.com/business/Industry/export-ban-on-rice-is-regulation-rather-than-restriction-for-food-security-india-to-wtos-agriculture-committee-meet/article67356967.ece.
12 Mint, dated January 2, 2024.
13 Homi Bhabha, "Jawaharlal Nehru and the Bomb," *The Wire*, April 25, 2023. https://thewire.in/books/homi-bhabha-jawaharlal-nehru-and-the-bomb, accessed on January 27, 2024.
14 Minhaz Merchant, "Did Nehru Refuse Kennedy's Nuclear Weapons Technology Offer?," *Dailyo*, 15 July 2016. https://www.dailyo.in/politics/did-nehru-refuse-kennedys-nuclear-technology-offer-nsg-china-11779.
15 US Intelligence and the Indian Bomb, "National Security Archive (George Washington University," Electronic Briefing No. 187, edited by Jeffrey Richelson, released on April 13, 2006. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB187/index.htm.
16 Gopalaswami Parthasarathi **(**July 7, 1912–August 1, 1995), often known simply as GP, was an Indian journalist, educationist, and diplomat who held several important positions including India's Ambassador to China and served as Permanent Representative to the United Nations from August 1965 to December 1968.
17 Bhakhtiar K. Dadabhoy. 2023. *Homi J. Bhabha—A Life*. New Delhi: Rupa Publications.
18 Office of the Historian, US State Department, The Nuclear Non-Proliferation Treaty (NPT), 1968—Milestones: 1961–1968—Milestones in the History of US Foreign Relations—Office of the Historian (state.gov). Accessed on February 19, 2024. https://history.state.gov/milestones/1961-1968/npt.
19 Office of the Historian, US State Department, The Nuclear Non-Proliferation Treaty (NPT) 1968—Milestones: 1961–1968—Milestones in the History of US Foreign Relations—Office of the Historian (state.gov). Accessed on February 19, 2024.
20 Article IX(3) of the NPT can be accessed at UNODA Treaties Database.
21 Articles I to IV of the NPT, can be accessed at UNODA Treaties Database.
22 India Nuclear Overview, NTI Fact Sheet, November 4, 2019 (India Nuclear Overview. https://www.nti.org/countries/india/. Accessed on February 19, 2024.
23 India's Nuclear Weapons Program—Smiling Buddha: 1974 (nuclearweaponarchive.org).
24 The Brasstacks Crisis, Center For Arms Control and Non-Proliferation, November 16, 2022. https://armscontrolcenter.org/the-brasstacks-crisis. Accessed on April 25, 2024.
25 The Print, February 10, 2024. https://theprint.in/walk-the-talk/this-secret-will-perish-with-me-when-narasimha-rao-was-asked-if-india-delayed-nuclear-test/1961746/. Accessed on April 25, 2024.
26 BJP Election Manifesto 2014, p. 17. www.bjp.org/manifesto2014. Accessed on April 25, 2024.

27 NDTV, August 16, 2019, India's No First Use Nuclear Policy: Explained in Five Points. ndtv.com. Accessed on April 25, 2025.
28 India–US Joint Statement, July 18, 2005 (issued on the occasion of PM Dr Manmohan Singh Visit to the USA). Ministry of External Affairs website.
29 Department of Space Press Release dated February 10, 2022 release by Press Information Bureau (pib.gov.in). Accessed on April 27, 2024.
30 BBC, August 23, 2023.
31 Taking India's Cost-Effective Space Launches to Next Level by Rajeswari Pillai Rajagopalan, *The Diplomat*, October 30, 2021. https://thediplomat.com/2021/10/taking-indias-cost-effective-space-launches-to-the-next-level/. Accessed on April 26, 2024.
32 EY(India) report titled "India @100: Realizing the potential of a US$26 trillion economy." https://www.ey.com/content/dam/ey-unified-site/ey.com/en-in/newsroom/2023/1/documents/ey-india-at-100-full-version.pdf#:~:text=India%40100%3A%20Realizing%20the%20potential%20of%20a%20US%2426%20trillion,economy%20after%20China%20and%20the%20US%20by%202030.version.pdf#:~:text=India%40100%3A%20Realizing%20the%20potential%20of%20a%20US%2426%20trillion,economy%20after%20China%20and%20the%20US%20by%202030.

Bibliography

Chand, R., & Singh, J. 2023, July. *From green revolution to Amrit Kaal*. NITI Ayog. https://www.niti.gov.in/sites/default/files/2023-07/Aggricultrue_Amritkal.pdf

EY. n.d. *INDIA@100: Realizing the potential of a $26 trillion economy*. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/newsroom/2023/1/documents/ey-india-at-100-full-version.pdf

India and Pakistan Archives. 2022, November 16. *The Brasstacks Crisis*. Center for Arms Control and Non-Proliferation. https://armscontrolcenter.org/asia/india-pakistan/page/2/

India Nuclear Overview. 2021, October 5. The Nuclear Threat Initiative. https://www.nti.org/analysis/articles/india-nuclear/

Jacob, J. 2019, August 16. *What is India's "no first use" nuclear policy: Explained in five points*. www.ndtv.com. https://www.ndtv.com/india-news/indias-no-first-use-nuclear-policy-explained-in-five-points-2086126

Merchant, M. 2016, July 15. *Did Nehru refuse Kennedy's nuclear weapons technology offer?* Daily. https://www.dailyo.in/politics/did-nehru-refuse-kennedys-nuclear-technology-offer-nsg-china-11779

Ministry of Commerce. 2021, December 31. *In April–October (2021–22) period, India's wheat exports surpassed $ 872 million from only $135 million achieved in April-October (2020–21) and set to achieve an all-time record shipment in the current financial year*. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1786624

Ministry of Commerce. 2023, July 14. *India's foreign trade: June 2023* (Press Release) https://commerce.gov.in/wp-content/uploads/2023/07/Press-Release-June-2023-f.pdf

Pandey, G. 2023, July 14. Chandrayan-3's success: ISRO's 9 upcoming missions of 2023 and beyond. *BBC News*. https://timesofindia.indiatimes.com/gadgets-news/chandrayan-3s-success-isros-9-upcoming-missions-of-2023-and-beyond/photostory/103072174.cms

Perkovich, G. 2000. Bhabha's quest for the bomb. *The Bulletin of the Atomic Scientist* 56(3), 54–63. https://journals.sagepub.com/doi/pdf/10.2968/056003012

Press Information Bureau. 2022, February 10. *Department of space press release*. https://pib.gov.in/PressReleseDetail.aspx?PRID=2106162

Press Information of Bureau. 2022, June 5. *Ministry of consumer affairs, food & public distribution*. Government of India. https://consumeraffairs.nic.in/more/press-release

PTI. 2023, September 28. Export ban on rice is regulation rather than restriction for food security: India to WTO's Agriculture Committee Meet. *The Hindu*. https://www.thehindu.com/business/Industry/export-ban-on-rice-is-regulation-rather-than-restriction-for-food-security

Rajagopalan, R. P. 2023, December 4. *Taking India's cost-effective space launches to the next level*. orfonline.org. https://www.orfonline.org/research/taking-indias-cost-effective-space-launches-to-the-next-level

Smiling Buddha: 1974. 2001, November 8. India's Nuclear Weapons Program – Smiling Buddha: 1974. https://nuclearweaponarchive.org/India/IndiaSmiling.html

The Print. 2024, December 20. *'This secret will perish with me' – when Narasimha Rao was asked if India delayed nuclear test*. https://theprint.in/walk-the-talk/this-secret-will-perish-with-me-when-narasimha-rao-was-asked-if-india-delayed-nuclear-test/1961746/

Treaty on the non-proliferation of nuclear weapons (NPT). United Nations Office for Disarmament Affairs. n.d. https://disarmament.unoda.org/wmd/nuclear/npt/text/

US Department of State. 1968. *The nuclear non-proliferation treaty (NPT) 1968*. US Department of State. https://history.state.gov/milestones/1961-1968/npt

US Intelligence and the Indian Bomb. 2006, April 12. *National security archive*, edited by Jeffrey Richelson, Electronic Briefing No187. George Washington University. https://nsarchive.gwu.edu/postings/all/full-list

Part II
Energy and Geopolitics

7 Southeast Asia in the Geopolitics of Green Transition

Great-Power Competition and Challenges

Mohd Faheem

Introduction

The transition from fossil fuels to clean energy is proving to be a complex process, fraught with geopolitical tensions. Despite growing greenhouse gas emissions and extreme weather events, at present the efforts to move beyond fossil fuels remain insufficient. The global energy crisis, exemplified by Europe's soaring electricity prices and China's urgent push for winter energy supplies, highlights countries' continued dependence on oil and gas. Major producers such as Russia and Saudi Arabia are leveraging their energy resources for geopolitical influence, while the US and other nations struggle with problems of energy security (Bordoff & O'Sullivan, 2022). While clean energy is expected to reshape geopolitics in future, the transition will be anything but smooth. Fossil fuel-dependent states may see short-term gains before they experience long-term declines, and developing nations will require vast energy supplies despite facing the most severe climate change effects. Clean energy itself will introduce its own new risks and uncertainties. Rather than slowing the transition, policymakers must recognize and manage the disruptions that will come with it. Failure to address the immediate challenges—such as energy security, affordability, and economic stability—could undermine public support and slow the shift toward a net-zero future. Though the use of fossil fuels may eventually decline, the politics of energy will persist. Today, anyone considering the world's energy future has to pay close attention to Southeast Asia, an economically dynamic region that has become an increasingly influential force in the global energy system.

As the world shifts from fossil fuels to clean energy, the geopolitical landscape will undergo profound changes, with influence no longer tied to oil reserves but focused on factors such as innovation, the control of critical minerals, and supremacy in clean energy technologies. The transition process will differ significantly from the end state, and while traditional energy powers may lose some influence, new forms of dominance will emerge.

Clean energy technologies rely heavily on critical minerals such as cobalt, lithium, copper, nickel, and rare earth elements. Demand for these minerals is expected to surge sixfold by 2040. A small number of countries currently

DOI: 10.4324/9781003633204-9

dominate supplies of these materials—the DRC (cobalt), Australia (lithium), and China (rare earths)—giving them significant geopolitical leverage. China's dominance extends beyond mining to processing and refining, further strengthening its influence. The ability to manufacture clean energy components cheaply will be another key factor in this future. China is the leader in the production of solar power components, including 90% of semiconductor wafers and two-thirds of the world's polysilicon. While China's control over supply chains can cause disruptions, such as bottlenecks and price spikes, it does lacks the immediate, life-or-death leverage that oil-exporting countries historically wielded. Over time, market forces will likely diversify production and reduce dependency on any one single supplier. The clean energy transition will push back against globalization. A decarbonized world will rely more on locally produced electricity, reducing energy-related trade. Protectionism can also be seen to be on the rise as countries impose tariffs to protect domestic clean energy industries, such as India's duties on Chinese solar panels. Additionally, climate-related economic statecraft, like the EU's carbon border adjustments, may lead to global trade fragmentation. Over the next three decades, the clean energy transition will require an extra $100 trillion in capital expenditures and a total overhaul of the world economy. It is unlikely that such a drastic change can be carried out in a well-organized, controlled, and seamless manner. Indeed, even if there were a master designer creating the intricately linked global energy system, an orderly transition would be difficult enough. Obviously in this case there isn't one.

The nations of the Association of Southeast Asian Nations (ASEAN) are on track to rank among the top five economies in the world by 2030 following two decades of impressive economic expansion. With a population of over 720 million, Southeast Asia is also expected to house more than one-twelfth of the global population at that time. This area is ready to solidify its status as a major energy producer. Southeast Asia alone is responsible for 25% of the rise in global energy demand through 2035; by 2050, it is expected to overtake EU consumption as a whole. Southeast Asia's strategic location along important maritime routes, expanding energy demand, and abundance of natural resources make it a unique player in the global energy transition. The area is turning becoming a crucial theater of conflict for power as the world transitions from fossil fuels to renewable energy. Southeast Asia is a crucial area of emphasis for the policies of great powers, especially the US and China, who are fighting for supremacy in rare earth resources, renewable energy technology, and infrastructure projects. The issues of energy security, regional collaboration, and sustainable development are highlighted in this chapter's analysis of the great-power competition's effects on Southeast Asia's green transition.

Southeast Asia's Role in the Green Transition

Southeast Asia's natural environment contains a wealth of natural resources that have been turned into energy assets. These include renewable energy sources such as solar, wind, hydro, geothermal, and bioenergy resources, as

well as fossil energy sources like coal, oil, and gas, and also important mineral reserves. Fossil energy sources in Southeast Asia typically come from relatively recent geological formations (from around 50 million years ago to the present) made up of sediments rich in organic matter that were formed in shallow marine or terrestrial settings.

Southeast Asia is rich in natural reserves of critical minerals, such as nickel and rare-earth elements. Today, Indonesia and the Philippines are the world's two largest producers of nickel, together accounting for about 65% of global mined production. Myanmar is the second-largest producer of rare earths and—together with Lao PDR, Thailand and Vietnam—makes up 20% of global production. To enable the mining of unexplored reserves throughout the region, a significant investment is required. Large potential for renewable energy sources such as solar, wind, hydro, geothermal, and biofuels are also present in the region's resources. Furthermore, Southeast Asia's tropical environment makes it a region with abundant bioenergy resources. Although palm oil feedstock accounts for almost all biofuel production in Malaysia and Indonesia, the region also has access to significant amounts of urban trash and agricultural and forestry wastes.

Renewable energy is becoming increasingly popular in Southeast Asia, and solar and wind energy are two of the main drivers of this change. Growing energy demands, climate change pledges, and the need to lessen reliance on fossil fuels are the main drivers of this transformation. However, because of variations in economic forces, geographic conditions, and policies, progress differs from nation to nation. In Southeast Asia, especially in Vietnam, Thailand, Malaysia, and the Philippines, solar energy has grown rapidly. With more than 16 GW of installed solar power as of 2022, Vietnam is the area leader, largely due to alluring government incentives such as feed-in tariffs (FiTs).

Under its Alternative Energy Development Plan (AEDP), Thailand made significant investments in rooftop solar projects and large-scale solar farms, making it an early adopter. Countries such as Indonesia and the Philippines have vast solar potential due to high solar irradiation, but progress has been slower due to regulatory hurdles and financing challenges. One emerging trend in the region is the development of floating solar farms, especially in land-scarce countries like Singapore, which has launched one of the world's largest floating solar projects at the Tengeh Reservoir.

While not as advanced as solar, wind energy is gaining momentum, especially in Vietnam, which has some of Southeast Asia's best wind resources. At present, Vietnam has over 4 GW of installed wind capacity, both onshore and offshore, with plans for further expansion under its energy roadmap. Thailand and the Philippines are also investing in wind energy. The Philippines is home to Southeast Asia's first wind farm, the Bangui Wind Farm in Ilocos Norte. However, countries such as Indonesia and Myanmar face challenges due to inconsistent wind patterns, complex terrains, and underdeveloped infrastructure.

Southeast Asia is attracting significant foreign investments from countries like China, Japan, South Korea, and European nations. Public–private partnerships (PPPs) are driving large-scale projects, while advancements in energy storage,

smart grids, and floating solar technology are addressing key technical challenges. The region's solar and wind capacity is expected to triple by 2030, with Vietnam, Thailand, and the Philippines leading the growth. Offshore wind projects are also gaining traction, particularly in Vietnam and the Philippines, due to favorable coastal conditions. Additionally, there's a growing focus on decentralized energy systems, including rooftop solar and mini-grids for remote areas.

Strategic Importance of Southeast Asia

Southeast Asia holds significant strategic importance due to its geopolitical location, economic potential, maritime relevance, and cultural diversity. Its position at the crossroads of the Indian and Pacific Oceans makes it a vital hub for global trade, security, and political influence. Southeast Asia's location connects East Asia, South Asia, and Oceania, making it crucial for global power dynamics. The region controls key maritime chokepoints, notably the Strait of Malacca, through which a significant portion of the world's trade and energy supplies pass. This has led to intense interest from global powers, as control over these routes directly impacts international commerce and strategic security (Acharya, 2021). Southeast Asia's rapidly growing economies, such as Indonesia, Vietnam, Thailand, and Malaysia, contribute significantly to global supply chains in sectors like electronics, agriculture, textiles, and natural resources. The region's economic strength is bolstered by ASEAN, which fosters regional cooperation and plays a major role in global trade agreements like the Regional Comprehensive Economic Partnership (RCEP). Additionally, Southeast Asia is a magnet for foreign investments due to its young workforce, rapid urbanization, and technological advancements, positioning it as a key driver of the global economy.

The region is pivotal to global maritime security due to the South China Sea, a contested area rich in oil, gas, and fisheries. The disputes in this area involve several countries, including China, Vietnam, the Philippines, Malaysia, and Brunei, raising concerns about freedom of navigation. This has attracted military interest from global powers like the US, China, India, and Japan, resulting in military partnerships, naval exercises, and defense agreements to secure their strategic interests in the region. Southeast Asia is known for its cultural diversity, with a rich mix of ethnicities, languages, and religions that influence global cultural dynamics. The region's vibrant traditions and historical landmarks make it a major tourism hub, attracting millions of visitors to destinations like Bali, Angkor Wat, Bangkok, and Ha Long Bay. This cultural richness also enhances the region's soft power on the global stage.

Great-Power Roles in Green Transition in Southeast Asia

Southeast Asia is a focal point in the strategic rivalry between global powers, particularly the US and China. China's Belt and Road Initiative (BRI) and the US's Indo-Pacific Strategy reflect their competing interests in the region.

China's Role in Green Transition in Southeast Asia

For a number of important reasons, including its economic clout, technological leadership, investment potential, and geopolitical strategy, China is a major force in Southeast Asia's green transition. As the biggest emitter of greenhouse gases in the world, China has a stake in lowering its carbon footprint and promoting the development of clean energy globally, particularly in an economically important region like Southeast Asia. With strong economic connections throughout the area, China is Southeast Asia's biggest commercial partner. One of the main channels for encouraging investments in green energy is its BRI, which seeks to link nations through infrastructural projects. China has funded and carried out a large number of renewable energy projects (such as wind and solar power) throughout Southeast Asia under the BRI, which is in line with China's long-term green energy objectives as well as those of the region. By supplying the required technology, funding, and experience, China's investments in infrastructure—such as solar farms, hydropower plants, and smart grids—assist Southeast Asia in its transition to green energy.

China leads the world in green energy technologies, particularly in the areas of energy storage, wind, and solar power. It is the biggest producer of wind turbines and solar panels in the world, and it exports both to Southeast Asia and other countries. It is also the biggest provider of photovoltaic (PV) cells due to its dominance in the solar panel manufacturing industry. With its enormous solar potential, Southeast Asia gains substantially from cheap Chinese solar technology, which makes it possible for nations there to increase their solar capacity. Additionally, the country is a major manufacturer of wind turbines and related equipment. Its increasing emphasis on offshore wind technology directly affects nations with significant offshore wind potential, such as the Philippines and Vietnam.

China is also one of Southeast Asia's main sources of foreign direct investment (FDI). It can finance large-scale green energy projects that many Southeast Asian nations might not be able to pay on their own with the support of state-owned businesses and major Chinese corporations. This is crucial as many countries in Southeast Asia are still switching from dirty energy sources such as coal to greener alternatives like solar and wind. Solar parks and hydropower facilities are among the many renewable energy projects in Southeast Asia that China has financed through development banks such as the Export–Import Bank of China and the China Development Bank (CDB).

China's green diplomacy has had a significant influence on Southeast Asia's green transition. By taking the lead in the global fight against climate change, China expands its geopolitical influence in the region. It offers green technology, capital, and expertise as part of its broader geopolitical objectives. Through green energy partnerships, China strengthens its political and economic ties with Southeast Asian countries and advances its standing as a responsible global leader. China is progressively incorporating green technologies into its worldwide supply chains as it moves toward a greener economy of its own.

Since China's supply of green energy equipment and materials is essential to the region's energy transition, Southeast Asia gains from this integration. The nations in the region can expand their renewable energy initiatives by integrating Chinese green energy technologies into local markets, guaranteeing access to high-quality technology at competitive prices.

The United States' Role in Green Transition in Southeast Asia

The United States plays a significant role in Southeast Asia's green transition, both through direct investments in renewable energy projects and by promoting sustainable development policies. The US has been a major supporter of clean energy initiatives in the region, using its technological expertise, financial resources, and diplomatic influence to foster green growth in Southeast Asia.

In Southeast Asia, the United States is a major source of FDI, especially in the renewable energy industry. Large-scale renewable energy initiatives using solar, wind, bioenergy, and energy storage are being undertaken by American businesses. The United States offers grants, loans, and technical assistance for green energy projects through organizations such as the US Agency for International Development (USAID). The goal of initiatives like the Asia EDGE (Enhancing Development and Growth through Energy) program and the US–ASEAN Smart Cities Partnership is to assist Southeast Asian nations in making the transition to more sustainable energy systems. From wind farms in the Philippines to solar power in Vietnam and Thailand, major US corporations like General Electric (GE) and First Solar have made investments in renewable energy projects around the region. These businesses provide local markets with cutting-edge technology and managerial know-how.

Southeast Asia's green shift has accelerated thanks in large part to the US's leadership in clean energy innovation and its knowledge in solar, wind, energy storage, and smart grids. American businesses rank among the world's biggest suppliers of wind turbines and solar panels. As a result, innovative renewable energy technology created in the United States are advantageous to nations like Vietnam, Thailand, and Indonesia. In order to integrate intermittent renewable sources like solar and wind into the grid, US companies are also at the forefront of energy storage technology. Better energy management and efficiency are made possible by the US's funding for Southeast Asia's smart grid development.

The US government seeks to promote sustainable energy policy reforms in Southeast Asia through programs such as the Clean Energy Ministerial (CEM) and its involvement in the International Renewable Energy Agency (IRENA). In order to create national renewable energy action plans, assist in establishing energy objectives, and establish clean energy regulatory frameworks, the United Nations collaborates with ASEAN member nations. One instance of US assistance for clean energy policies in the area is the US–ASEAN Clean Energy Program. In order to address concerns about energy security and promote the use of clean technology, the program helps design

energy policies and regulations. By supporting low-carbon solutions and funding programs targeted at lowering greenhouse gas emissions, the United States, a key participant in international climate agreements like the Paris Agreement, assists Southeast Asia in meeting global climate objectives.

The United States use climate diplomacy as a means of fortifying its ties with nations in Southeast Asia. The United States increases its influence in a strategically significant region by providing clean energy solutions and promoting environmental objectives. The United States is also using this tactic to thwart China's increasing influence in Southeast Asia's green transition. SEAETI, which was started by the United States in collaboration with Southeast Asian countries, aims to assist these countries in their transition to sustainable energy while fostering economic growth and stability in the area.

Access to electricity is a problem in many Southeast Asian nations, particularly in rural and isolated places. The United States has participated in initiatives aimed at boosting energy security, expanding energy access, and offering renewable energy alternatives to off-grid populations. In underprivileged areas, USAID has funded initiatives to increase the number of solar mini-grids and solar residential systems, enhancing access to power and lowering dependency on dirty diesel generators. By encouraging the diversity of energy sources, the United States also advances energy security in Southeast Asia. As part of their energy security plans, this involves urging nations to invest in renewable energy sources and lessen their reliance on fossil fuels.

To support sustainable energy initiatives in Southeast Asia, the United States collaborates closely with other nations and regional institutions, including the World Bank and Asian Development Bank (ADB). These partnerships enable large-scale renewable energy projects that could otherwise be beyond of the grasp of individual nations by combining resources, knowledge, and capital. In order to combat climate change and advance sustainable energy development in the area, the United States supports public–private partnerships that bring together governments, businesses, and international organizations.

Because of its proximity to China and its abundance of natural resources, particularly nickel, Southeast Asia has benefited from the US–China green competition. In order to lessen their reliance on China and take advantage of the region's affordable labor and manufacturing costs, major corporations from Korea, Japan, and the US are friend-shoring and near-shoring their supply chains to Southeast Asia. As a way of reducing their products' vulnerability to US protectionist trade duties, Chinese businesses are also moving their supply chains to the area, which they view as a "buffer zone." For example, they aimed to take advantage of Southeast Asia's two-year exemption from US solar tariffs, which expired in June 2024. Significant Chinese solar investments have been made in Cambodia, Malaysia, Thailand, and Vietnam, four countries which, in 2023, provided more than 75% of US imports of solar modules. The two biggest producers of nickel worldwide, Indonesia and the Philippines, are examples of crucial mineral-producing nations in which both the US and China are investing. In an effort to counter China's hegemony in nickel processing in

Indonesia, Washington has proposed a number of investment options, including joining the Mineral Security Partnership, a framework that aims to build critical-mineral supply chains between the US and its allies, and entering into a limited critical-mineral free-trade agreement that could be modeled after a US–Japan agreement. Although the Philippines' nickel deposits are of interest to both the US and China, no firm proposals have surfaced as of yet. If tariff constraints cause China's access to American and European markets to narrow, Southeast Asia may emerge as a desirable destination for eco-friendly goods. The market potential of the region has already been strengthened by the many electric vehicle (EV)-adoption incentives offered by regional governments. For instance, Thailand and Indonesia have implemented exclusions from import duties and corporation taxes. Companies with headquarters in the US, like Tesla, and China, like BYD, are both looking to increase their market share in the area.

Green Geopolitical Challenges

Southeast Asian nations are increasingly including green transition objectives in their foreign policy agendas as the US–China green competition intensifies. For example, the May 2023 announcement by ASEAN leaders indicated a concerted effort to further establish the area as a worldwide center for EV manufacturing. This goal has been reaffirmed in subsequent high-level ASEAN meetings and declarations. Green-transition plans and pledges are also becoming more and more important in bilateral agendas between Southeast Asian nations and the US and China. The US–China competition poses two obstacles to the green transformation of Southeast Asian nations. An initial challenge is to promote green growth. For instance, the US is closely examining supply-chain relocations for solar modules to the region because of its concern that the area is turning into a conduit for Chinese goods. This has led Chinese solar businesses, such as Longi, to contemplate halting or postponing their manufacturing plans.

Southeast Asian nations must maintain their attractiveness as geopolitically neutral economic partners free from great-power dominance in order to overcome this obstacle. Some governments in Southeast Asia could turn to ASEAN to regulate intra-regional rivalry, such as in the EV market, and to persuade big powers of the value of increasing the region's strategic autonomy. To avoid being overly reliant on any one party, others might want to concentrate on embracing a variety of investing partners. For example, Indonesia is working with nations like Korea to lessen Chinese control in its rare-earth mining and processing industries.

How Southeast Asian nations use the current influx of foreign investment to generate long-term value—particularly in relation to domestic technology capacity—is the second challenge they face. Promoting businesses' long-term localization in the area is becoming a crucial component of Southeast Asian nations' geo-economics strategies as geopolitical challenges pose a growing danger to green supply-chain relocations.

By collaborating with Geely Auto of China, the Malaysian automaker Proton has attempted this strategy, giving the latter access to the local market while enabling the former to improve its products with cutting-edge technologies. With the goal of controlling a comprehensive supply chain for EV production, Indonesia has reaffirmed its commitment to its nickel-export prohibition in order to encourage downstream investments, such as in the production of batteries and nickel intermediary products. For its part, China appears to have recognized the advantages of promoting EV localization in order to allay US worries. States in Southeast Asia could take advantage of this trend and communicate localization requirements to other pertinent businesses in addition to the EV sector, even if their weak investment-screening procedures may eventually make them vulnerable to exploitation.

Conclusions

Southeast Asia's strategic significance stems from its pivotal position in international commerce, security, and economic development. The area continues to play a significant role in international politics in the 21st century due to its control over vital sea routes, thriving economies, cultural impact, and participation in great-power rivalries. Solar and wind energy have enormous promise in Southeast Asia. While nations like Thailand and Vietnam are spearheading the shift, others are confronted with obstacles pertaining to funding, regulatory frameworks, and infrastructure. Policy changes, technology advancements, and regional collaboration will be essential to maximizing the region's potential for renewable energy. In the framework of great-power competition, Southeast Asia's green transition offers both possibilities and problems.

Although the region has a lot of promise due to its resources and strategic location, a sustainable and inclusive energy future depends on managing internal vulnerabilities and navigating geopolitical conflicts. Southeast Asia has the potential to become a leader in the global green transition by promoting regional collaboration and balancing outside pressures. There will be geopolitical winners and losers from the shift. Russia faces long-term economic concerns because of its reliance on the export of fossil fuels, while the United States and China stand to gain from their technical superiority and resource management. Future alliances and wars may be shaped by growing tensions between major countries over resource access, supply networks, and climate policy. In the end, rivalry and conflict will always arise throughout the shift, even though collaboration is crucial to reaching net-zero goals.

China's economic might, technical innovations, financial backing, and geopolitical approach have all contributed to its supremacy in Southeast Asia's green transformation. In addition to spearheading the transition to renewable energy, China, a significant regional partner, is establishing itself as a worldwide leader in sustainable development, which will aid the area and its own environmental goals. The United States contributes in several ways to Southeast Asia's green transition, including through policy advocacy, technological transfer, financial support, and climate diplomacy. Although China is a rival, especially

when it comes to funding and infrastructure development, the United States concentrates on offering cutting-edge technology, knowledge, and long-term sustainability solutions that support the area in achieving its climate and renewable energy targets. The United States is anticipated to continue to play a significant role in influencing Southeast Asia's clean energy landscape as the region transitions to a more environmentally friendly future. Although the US policy places a strong emphasis on openness and democratic government, it finds it difficult to match China's investment level. China and the United States vie for market share in Southeast Asia's green energy sector. The United States concentrates on technology transfer, policy development, and climate funding, especially in areas like climate resilience and adaption methods, whereas China provides substantial financial and infrastructural expenditures.

Bibliography

Acharya, A. 2021. *ASEAN and regional order: Revisiting security community in Southeast Asia*. Routledge.

Bian, L., Dikau, S., Miller, H., Pierfederici, R., Stern, N., & Ward, B. (2024). China's role in accelerating the global energy transition through green supply chains and trade. *London School of Economics and Political Science, Grantham Research Institute on Climate Change and the Environment, and Energy Foundation China*, *Policy Insight*.

Bordoff, J., & O'Sullivan Meghan, L. 2022. Green upheaval: The new geopolitics of energy. *Foreign Affairs*, *101*: 68.

Li, B., Nian, V., Shi, X., Li, H., & Boey, A. 2020. Perspectives of energy transitions in East and Southeast Asia. *Wiley Interdisciplinary Reviews: Energy and Environment*, *9*(1): e364.

Shambaugh, D. 2020. *Where great powers meet: America & China in Southeast Asia*. Oxford University Press.

Umbach, F. 2021. *Strengthening energy security and building resilience in the Asia–Pacific*. United Nation Publications.

Yurnaidi, Z., Supasa, T., Shani, N., Fuqoha, I., Kim, S., & Min, E. 2024. State of energy security in East and Southeast Asia. In *The water, energy, and food security Nexus in Asia and the Pacific: East and Southeast Asia*: 63–82. Springer Nature Switzerland.

8 Developing Nepal as a Hydrogen Hub for Contributing to the Energy Transition and Green Growth in South Asia

Biraj Singh Thapa and Bishnu Pandey

Introduction

It has been estimated that renewable energy will contribute up to 85% of the power sector by 2050, with an increase of 25% in 2017 (International Renewable Energy Agency, 2022). The swift development of the global renewable energy landscape is due to the commitment of nearly 140 countries, including major emitters China, India, the United States, and the European Union, to reach net zero carbon emissions between 2050 and 2070 (Intergovernmental Panel on Climate Change, 2022). As a result of these commitments, the investment in renewable energy surpasses fossil fuels by 0.7 trillion USD, reaching 1.8 trillion USD in 2022 (World Energy Investment, n.d.). Despite these efforts, average yearly atmospheric carbon dioxide (CO_2) levels hit a record high of 419.3 parts per million (ppm) in 2023 (GHG Emissions of All World Countries—Publications Office of the EU, n.d.).

The fuel types that accounted for the world's energy consumption in the year 2023 were 29.78% oil, 21.89% natural gas, 24.87% coal, and 13.69% renewables (Grubler et al., 2018). The electricity and heat generation sectors, followed by the transport sector, manufacturing and construction sector, agriculture sector, etc., are the major consumers of fossil-based fuels and significant emitters of greenhouse gases (Figure 8.1). Transitioning these sectors to renewable energy is challenging due to the deep-rooted reliance on traditional fuels and the resistance arising from the reliability, quality, and flexibility challenges associated with current renewable sources, despite promotional investments and taxation mechanisms. (Global Greenhouse Gas Emissions: 1990–2021 and Preliminary 2022 Estimates, n.d.)

The socioeconomic and environmental issues induced by emissions are more challenging in developing countries, where the GDP is low. As shown in Figure 8.2, South Asian nations such as Nepal, India, Bangladesh, Pakistan, and Afghanistan experience much higher exposure to $PM_{2.5}$ air pollutants due to high dependencies on fossil-based fuels in energy-intensive sectors. This has added pressures and challenges to decarbonizing the South Asian economy by deploying action- and policy-oriented interventions by the respective governments.

DOI: 10.4324/9781003633204-10

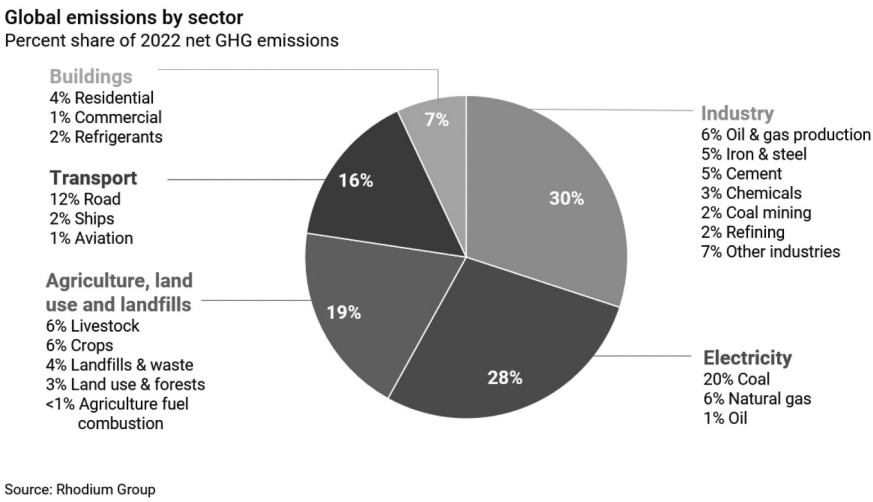

Figure 8.1 Greenhouse Gas Emission by sector (Global Greenhouse Gas Emissions: 1990–2021 and Preliminary 2022 Estimates, n.d.)

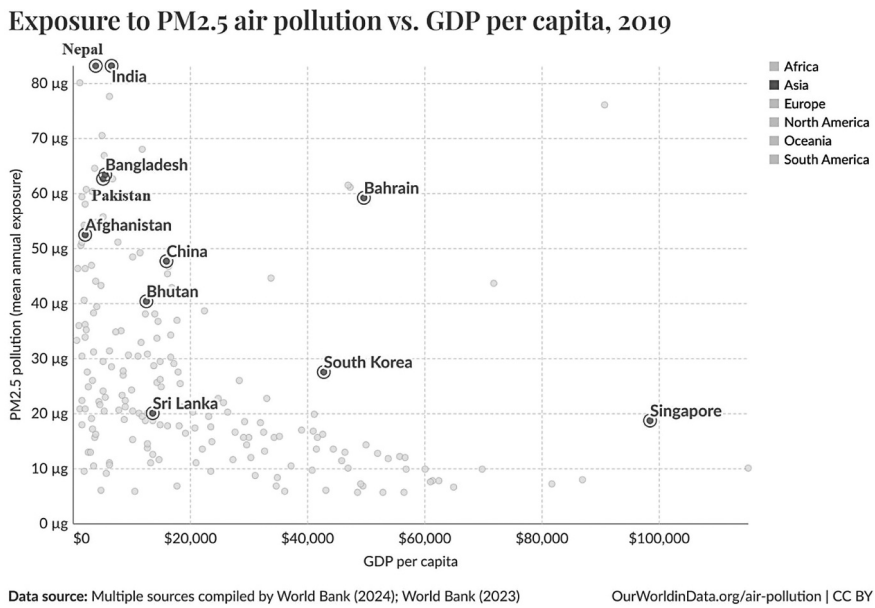

Figure 8.2 Per Capita CO_2 Emission (Ritchie et al., 2023).

Rising geopolitical pressure to increase the share of renewable energy in power generation has attracted significant investments to force energy transition and achieve climate goals. Remarkably, to date, no developed economies in Asia have moved their net zero targets earlier than midcentury to align with the Acceleration Agenda. Eight economies still lag behind the midcentury target. These include six that are aiming for 2060 (China, Bahrain, Indonesia, Kazakhstan, Kuwait, and Saudi Arabia), along with Thailand (2065) and India (2070). Instead, developing countries such as Pakistan and Bangladesh have committed to reducing carbon emissions by 50% and 21.8%, respectively, by the end of 2030. Likewise, Nepal and Sri Lanka have pledged rather ambitious goals of net zero emissions by 2045 and 2050, respectively. While these commitments have catalyzed the investments in the region, the dependency on fossil fuels is not decreasing. This makes the achievability of the climate targets difficult, despite the huge potential of renewable energy in Asia (Mitra et al., 2023).

Energy Consumption and Transition Scenario in the Asia Region

Energy supply and security are critical challenges for the achievement of energy independence and clean energy in South Asia. Many countries in this region depend on a single source to provide nearly 50% of their total electricity generation. At present, a number of countries are overly dependent on fossil-based sources, including Bangladesh (natural gas 53.86%; Shamim et al., 2022), India (coal 49.1%; (Electricity Generation in India 2023: Share of Different Sources, n.d. and Sri Lanka (oil 43%). The exception to this pattern is Nepal (hydropower 99.9%) (Naveed Iftikhar et al., 2015). The major sources of electricity generation in the South Asian countries are presented in Table 8.1.

Expanding renewables in developing countries is critical to meet growing energy demands and global decarbonization targets. In recent years, there has been a significant increase in renewable energy investments in Asian countries.

Table 8.1 Electricity Production Source of South Asian Countries (Energy Consumption in Pakistan, n.d.; Energy Consumption in Sri Lanka, n.d.; Naveed Iftikhar et al., 2015, Shamim et al., 2022)

Country	*Electricity Production Billion kilowatt-hours (kWh)*	*Coal (% of total)*	*Natural Gas (% of total)*	*Oil (% of total)*	*Renewable (% of total)*
India	1,452.43	49.7	6.1	0.1	40.9
Afghanistan	0.96743	–	–	–	–
Nepal	10,536	–	–	–	~100
Pakistan	109,7375	12.8	32.3	14.3	40.6
Sri Lanka	15,942	16		43	41
Bangladesh	6,238	5.62	53.86	27.18	1.32
China	12,158	33.9	–	–	53.9

As a result of China's energy transition commitments, its share of solar energy has jumped from nearly 0% in 2010 to 4% in 2014, reaching nearly 16% in 2023 (Renewable Energy Agency, 2023). Similarly, investments in renewable energy from other Asian countries, such as India, Japan, and the Republic of Korea, have also been significant over the decade (Renewable Energy Agency, 2023).

Despite this, the dependence on fossil fuels in these countries is significant. India and China, as the world's largest energy consumers, majorly depend on imported fossil fuels, as shown in Figure 8.3. In India, the production of petroleum and liquid fuel has remained steady, at near to 1 million barrels per day, whereas the consumption surged from under 2.5 million barrels per day in 2002 to approximately 4.5 million barrels per day in 2021. Over the next 20 years, India's import bill for fossil fuels is projected to triple, with oil accounting for the largest share. Moreover, the net dependence on imported oil is expected to rise above 90% by 2040. Similarly, in China, petroleum consumption increased from less than 5 million barrels per day in 2000 to approximately 15 million barrels per day in 2021, outpacing production and highlighting heavy reliance on imports of carbon-emitting fuels (Khan & Mumtaz, 2018). It is evident that both India and China would like to reduce the imports of petroleum products and substitute them with the import of green alternatives if opportunities are available.

Nepal has a large renewable energy potential with an estimated technically and economically feasible capacity of about 45,000 MW, yet the total installed

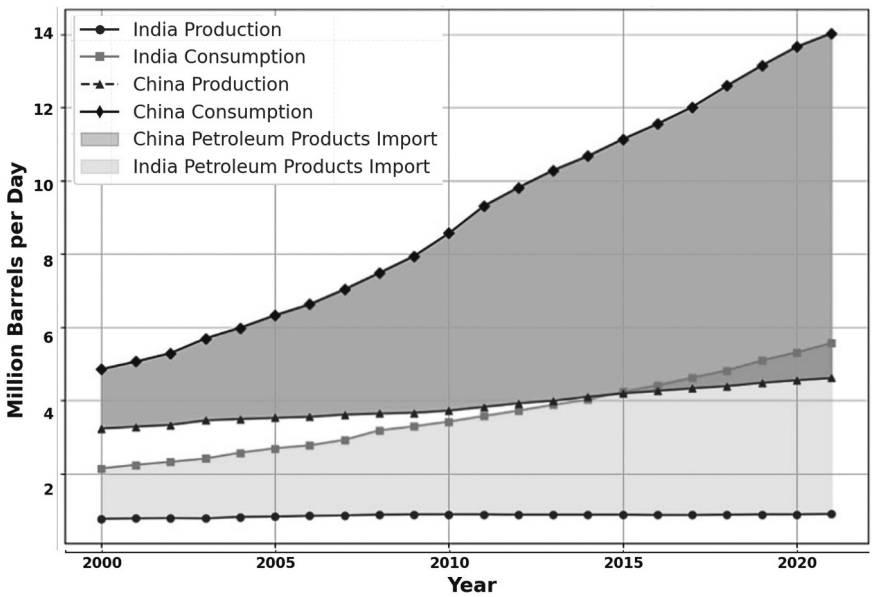

Figure 8.3 China and India Oil consumption and production million barrels/day (Adapted from (Energy Institute, 2024; Khan & Mumtaz, 2018)).

capacity as of 2024 stands at 3254 MW, predominantly from hydropower (Government of Nepal Water and Energy Commission Secretariat, 2023b). The government has made the roadmap and action plans to increase the electricity generation to 28,500 MW by 2035 (Electricity Regulatory Commission, 2024). This action plan will lead to the production of more than 18,000 MW of hydroelectricity curtailment. Demonstrating its interest in promoting a renewable energy mix and solar projects in the country, the Nepal Electricity Authority has initiated the process for a Power Purchase Agreement (PPA) for 900+ MW solar power projects (*Department of Electricity Development*, n.d.). Seasonal variations in hydroelectric production, influenced by the high flow during the rainy season and low flow in the dry season, present significant flexibility, quality, and reliability challenges (Marahatta et al., 2021). Nepal imports electricity during the dry season and exports its surplus during the wet season. In FY 2018/19, for example, Nepal imported 1543.28 GWh and exported 493.61 GWh (Nepal Electricity Authority, 2024). However, Nepal is expected to have a surplus of 18,000 MW in the wet season by 2035, making the management of the surplus a big challenge (Nepal Electricity Authority, 2024; Thapa et al., 2021). Due to active seismic zones and its challenging geography, the building of storage-based hydropower projects and pumped hydro-energy storage systems is difficult, and increasing infrastructure to consume energy in such a short period seems unachievable (Hosseini & Wahid, 2016). Extrapolating the current consumption trends to 2035 suggests Nepal will be able to consume approximately 10,200 MW of hydroelectricity by 2035. Consequently, due to the momentum of global climate change, there will be a pressing need for alternative solutions to balance the grid and effectively decarbonize Nepal's energy sector.

Green hydrogen is recognized as a zero-carbon energy source with great promise for future use as an energy carrier. Since green hydrogen is more adaptable and has a higher heat value (120–140 MJ/kg) than coal (20 MJ/kg) and gasoline (44 MJ/kg), it is expected to play a significant role in the global energy transition (Hosseini & Wahid, 2016). Green hydrogen presents a viable solution by leveraging surplus electricity during the wet season for production and storing it for re-electrification and other end-use applications (Hosseini & Wahid, 2016). It has been estimated that Nepalese Hydropower can produce 67,277 to 336,400 tons of green hydrogen using 20% and 100% surplus energy in 2030 (Thapa et al., 2021). Moreover, Nepal's newly endorsed Green Hydrogen Policy creates a supportive framework for attracting investments and enabling project development, aligning with the nation's aspirations for a sustainable energy transition ("Cabinet Approves Policy for Production and Use of Green Hydrogen," 2024).

Hydrogen Hubs for Energy Transition

A Hydrogen Hub is a large-scale initiative that focuses on the development of hydrogen production, distribution, and utilization infrastructure on a national or international level, typically powered by renewable energy, as shown in

Figure 8.4. The primary focus of a Hydrogen Hub is on creating a networked infrastructure capable of supporting the widespread adoption of hydrogen as a clean energy carrier across multiple industrial-scale applications. As of March 2024, there are more than 80 Hydrogen Hubs/valleys that support green energy have been established worldwide, with a cumulative investment of about EUR 30 billion for 30 global Hydrogen Valleys (*Hydrogen Valleys. Insights into the Emerging Hydrogen Economies around the World – Clean Hydrogen Partnership*, n.d.). The availability of renewable energy sources, mostly hydropower and solar, excessive consumption of imported fossil fuels, and geographic location between the economic giants make Nepal a favorable location for the development of Hydrogen Hubs. This study aims to introduce the framework of the Nepal Hydrogen Hub (NHH) for energy management and economic transformation in the country.

This vision integrates hydrogen production, storage, and utilization, facilitating the production of green ammonia, green urea, and green steel utilizing local resources to meet the local market demands in Nepal and explore export opportunities to the regional market. The study systematically examines the potential of renewable energy utilization for decarbonizing the industrial sector in Nepal. Special attention is given to leveraging Nepal's renewable energy and other resources to drive industrial decarbonization through green hydrogen technology within the envisioned Hydrogen Hub (Figure 8.4).

Nepal as a Hydrogen Hub

In 2022, Nepal's total energy consumption was recorded at 640 PJ. This is currently increasing at an annual rate of 4% (Government of Nepal Water and Energy Commission Secretariat, 2023a). Nepal's energy sources include biomass, petroleum products, coal, hydroelectricity, and renewable energy. While biomass consumption decreased from 66% in 2021 to 58.53% in 2022 (Government of Nepal Water and Energy Commission Secretariat, 2023a, 2023b), the consumption of petroleum products has been steadily increasing. Fossil fuel imports cost approximately 292.77 million USD in the year 2022, accounting for 14.1% of all imports into Nepal. Fossil fuels serve as the primary heating source in Nepalese industries, supplying approximately 65% of the total industrial energy (Government of Nepal Water and Energy Commission Secretariat, 2023b). Coal is the primary energy source for the industrial sector, mainly for heating and baking in the production and processing of brick, lime, cement, and steel. Due to population growth, inefficient operation, and increased economic production, it is expected that the demand for fossil fuels in Nepal will further rise in the coming years if strategic interventions are not implemented on time (Government of Nepal Water and Energy Commission Secretariat, 2023a). Figure 8.5 presents the hydroelectricity mapping of four envisioned Hydrogen Hubs, strategically located based on the different development stages of hydropower projects. NHH-I in Province 1 has a hydropower capacity of 5500 MW, while zones II, III, and IV have potentials of

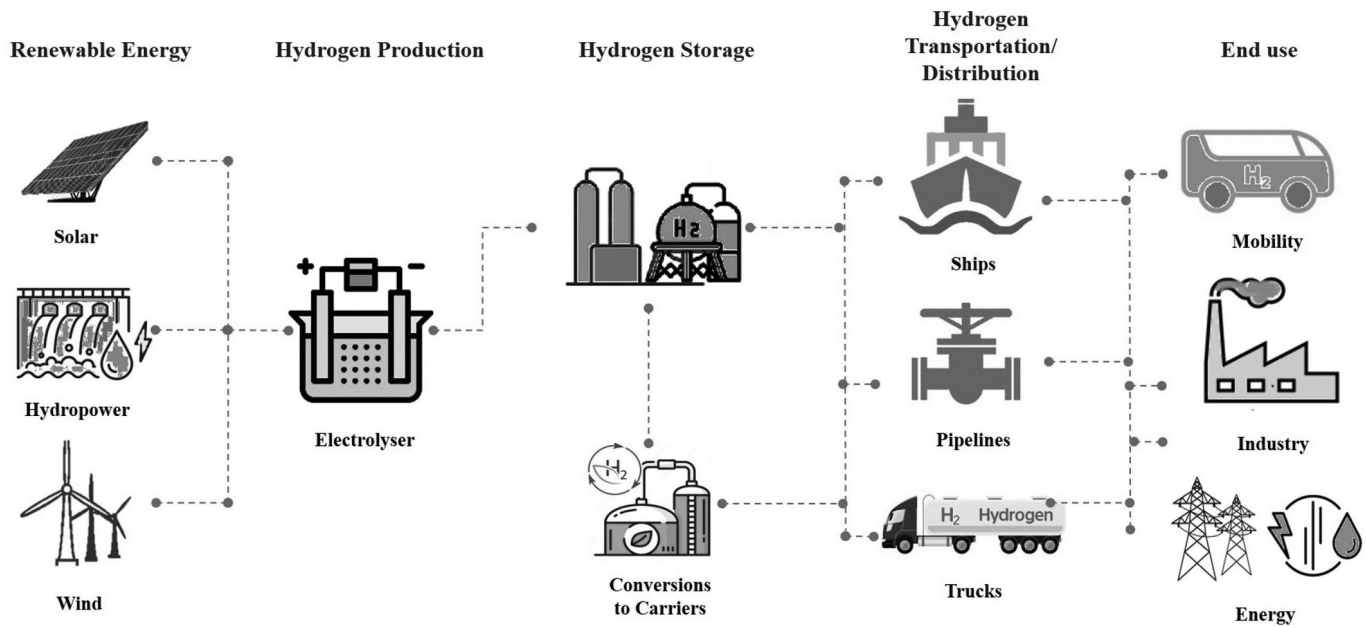

Figure 8.4 Green hydrogen value chain.

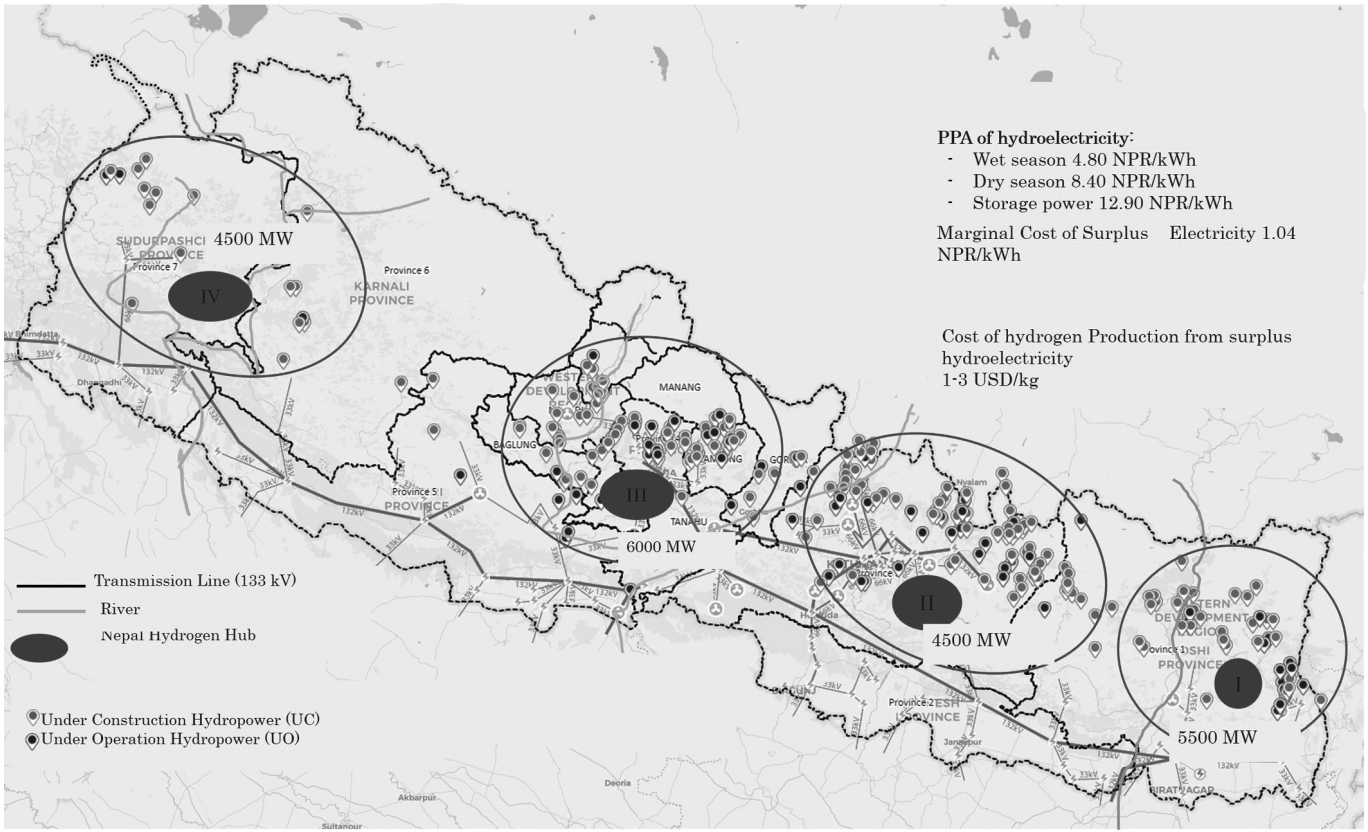

Figure 8.5 Hydroelectricity mapping for Nepal Hydrogen Hub (Adapted from (Marg et al., 2021; Nepal Electricity Authority, 2024; Water Resources and Energy Sectors, 2013).

4000, 6000, and 4500 MW, respectively. The capacity of each Hydrogen Hub is assumed to be one-third of the total installed hydropower. Each of the four proposed hubs has distinct objectives and advantages. Due to Nepal's strategic location, these Hydrogen Hubs have the potential to function as a collective hydrogen hub for a significant part of Asia. Hub I, situated near India, Bhutan, Bangladesh, and Myanmar, can leverage its location to facilitate hydrogen trade along the eastern corridor, particularly through ammonia transport. Hub II, located near China, offers strategic flexibility for hydrogen trade in that region. Hub III, positioned in central Nepal, holds significant potential for hydropower development and can function as a localized Hydrogen Hub, supporting domestic consumption through the production of green steel, cement, ammonia, urea, and other synthetic fuels as shown in Hub IV, with its strategic location in western Nepal, presents opportunities to explore hydrogen and ammonia trade possibilities with neighboring countries such as Pakistan, Afghanistan, and Tajikistan.

Figure 8.6 presents an overview of the proposed Nepal Hydrogen Hub. Green hydrogen can be produced using spilled or from a dedicated energy source comprising hydropower, solar, wind, or regional electricity. The produced hydrogen can be stored in various media and converted to electricity for grid stability, emergency power backup, and as a transportation fuel (Ghimire et al., 2024). Furthermore, the stored hydrogen can be utilized within specialized industrial zones for the production of high-value products such as green ammonia, green urea, green cement, and green steel. The produced green commodities can be consumed domestically in Nepal or exported to regional markets, primarily in the form of green ammonia. This centralized concept of green hydrogen production, storage, and end-use is envisioned as the Nepal Hydrogen Hub (NHH). This is expected to balance the regional power grid and enable the production and export of other clean energy derivatives to local and regional markets.

Methodological Framework

The calculation basis for estimating the demand for renewable energy and green hydrogen in NHH was projected for 2035. Figure 8.6 outlines the specific industrial applications of green hydrogen within the hub. The energy scenarios were studied using insights from relevant literature to assess the availability of renewable electricity for green hydrogen production.

Energy Demand Estimation

Process flows and energy consumption patterns within relevant industrial sectors were analyzed through extensive literature reviews, with a particular emphasis on heating and process-based applications. Energy demand across energy-intensive sectors, particularly that where direct electrification is challenging, was identified. Product demand was calculated using government

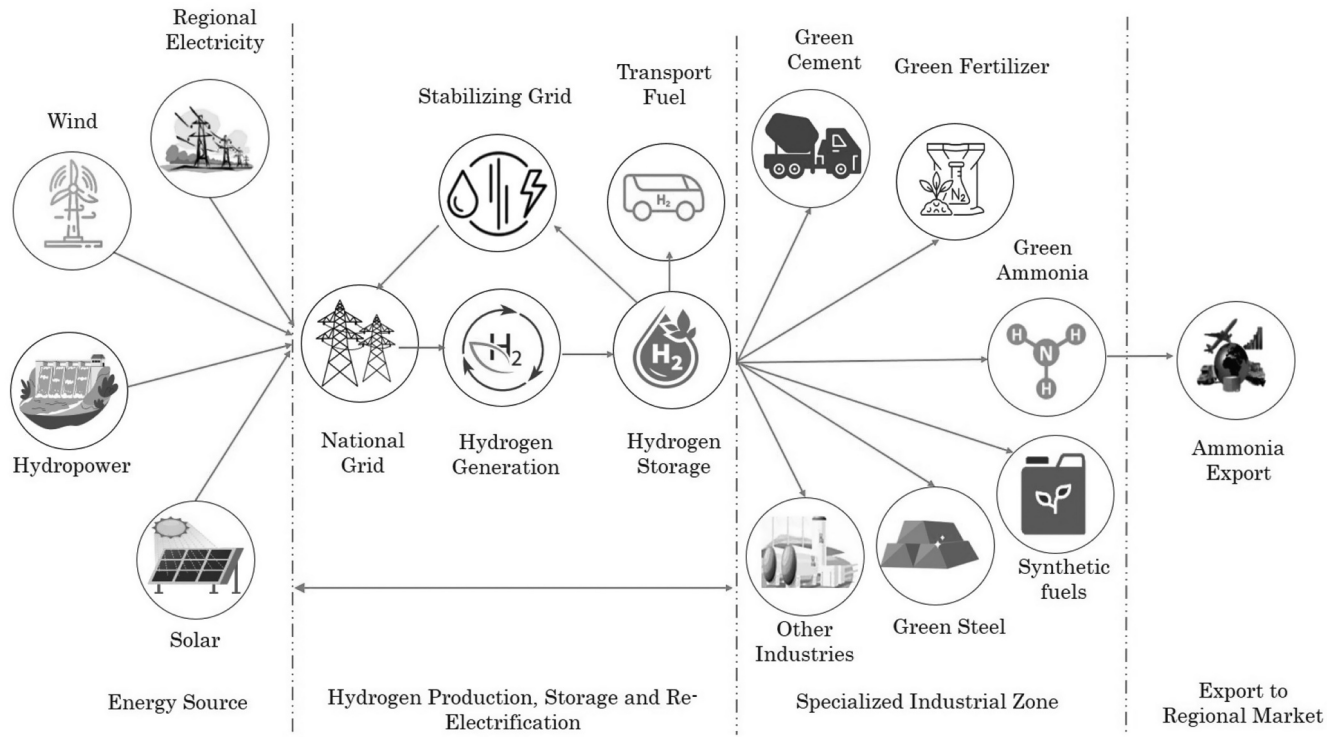

Figure 8.6 Outline of the Nepal Hydrogen Hub.

reports, the GDP contribution of the respective province to the country, and import data. Equivalent energy requirements were derived by converting fuel consumption data into energy units based on the calorific value of conventional fuels. The estimated demand for fertilizer assumes that the per-hectare needs of the agricultural land will remain stagnant. The total energy demand is categorized according to the nature of energy required, such as heating, process energy, or power for auxiliary processes. Green hydrogen is prioritized as a key decarbonization solution exclusively for hard-to-abate sectors and processes requiring high-temperature heating. Energy demand is predicted using the available mathematical models to ensure precise and sector-specific estimations (Turton, 2012).

Direct hydrogen utilization is emphasized for energy-intensive processes and direct feedstocks, including industrial heating and chemical applications. By aligning surplus renewable energy availability with sector-specific energy needs, the methodology provides a clear and robust pathway for the development of the Nepal Hydrogen Hub, supporting industrial decarbonization and the efficient utilization of renewable resources. Table 8.2 summarizes the methodological framework for the energy demand calculations.

The plant factor of 52.39% was taken as the reference for hydroelectricity production. (Nepal Electricity Authority, 2024).

Resources Mapping for Specialized Industrial Zone

The industrial sector of Nepal is a highly energy-intensive economy. The total consumption in this sector totals 144 PJ in Nepal, which is the second-most energy-intensive sector after the residential sector (395.7 PJ). Government of Nepal Water and Energy Commission Secretariat, 2023b). The major energy use in the industrial sector is for thermal applications. Consequently, coal is the most widely used fuel, accounting for 48.15%, followed by fuelwood at 16.83% (Government of Nepal Water and Energy Commission Secretariat, 2023b). With the adoption of new technologies, the use of electricity for thermal applications is increasing; however, the pace of replacing carbon-intensive technologies remains insufficient. Replacing all industrial processes with electricity poses further challenges due to the heating limitations of electric-based heating systems.

Traditionally iron making uses blast furnaces where coal is employed as a reducing agent to produce sponge iron, producing greenhouse gas up to 1.9 tons per ton of steel (Reccpedia Reccessary, n.d.). The production of green steel using H_2-DRI-based technology employs electricity as heating fuel, hydrogen as a reducing agent, and iron ore (Krüger et al., 2020). The emission is greatly reduced because water (H_2O) is the only by-product formed after the reaction inside the furnace. Moreover, Nepal has approximately 500 million metric tons of iron ore deposits, which can be processed with hydrogen as the

Table 8.2 Methodology for Energy Demand Estimations

S. N.	*Industrial sector*	*Method for product demand estimation for 2035*	*Method for energy demand calculation for a conventional process*	*The primary use of hydrogen for decarbonization*
1	Replace diesel-based transport	Demand forecast by the Water and Energy Commission Secretariat (Water Resources and Energy Sectors, 2013)	• Calorific value-based equivalent amount of energy released per liter of diesel consumed (Typical Calorific Values of Fuels - Forest Research, n.d.)	As a replacement for diesel used in the heavy-duty transportation sector (Shahzad & Iqbal Cheema, 2024)
2	Green ammonia and green urea	Demand forecast based on previous government reports and fertilizer needs per hectare of arable land (Ammonia Market Size, Share, Analysis, Report, n.d.; Planning & Development Cooperation Coordination Division, n.d.) (Chaudhary et al., 2022; Fertilizer Consumption (Kilograms per Hectare of Arable Land) | Data, n.d.)	• Balance of Plant Study for urea and ammonia (NH_3) production (Allen et al., 2021; Heath et al., 1985). • Energy demand estimation for ammonia production ((26 GJ of energy per ton of NH_3 production) (Rouwenhorst et al., 2020) • Energy requirement estimation for urea production (9.2 GJ of energy per ton of urea produced) (Rouwenhorst et al., 2020)	As feedstock consumables for the production process (Rouwenhorst et al., 2020)
3	Replace coal-based applications (cement, brick, boilers, others)	Demand forecast by the Water and Energy Commission Secretariat	• Calorific value-based equivalent amount of energy released per kg of coal consumed (Typical Calorific Values of Fuels - Forest Research, 2025)	As a replacement for coal in heating and process-based applications (A. Ghimire et al., 2023a, pp. 1–15)

4	Replacement of LPG for heat Applications	Demand forecast of LPG based on the Water and Energy Commission Secretariat (Water Resources and Energy Sectors, 2013)	• Calorific value-based equivalent amount of energy released per kg of LPG consumed (Typical Calorific Values of Fuels - Forest Research, 2025)	As a replacement for liquefied petroleum gas in heating applications (A. Ghimire et al., 2023a)
5	Iron ore reduction (green steel)	Demand forecast based on previous demand and linear regression demand forecast methods (Mahat et al., 2023)	• Balance of plant and energy calculations for the production of steel from iron Ore (11 TJ of energy is required for one ton of steel production in a Basic Oxygen Furnace using coal) (Energy Use in US Steel Manufacturing, n.d.) • Calorific value-based equivalent amount of energy released per liter of coal consumed in Cocking process (Typical Calorific Values of Fuels - Forest Research, 2025)	As an alternative fuel in cocking process (Coke Making | Industrial Efficiency Technology & Measures, n.d.)
6	Energy demand as base load for the associated (1-5) industrial sector	Study the Process (Czigler et al., 2020), (Pagani et al., 2024)	• Electricity is required for associated industrial processes.	
7	Export of Ammonia to the Regional Market	Study the Global Ammonia market and regional needs (Ammonia Market Size & Share Report)	• The Haber-Bosch process can be used to produce green ammonia for export using available energy after meeting the base load and energy requirement for the specialized industrial hub (1-6)	

reducing agent and hydroelectricity for heating (Mahat et al., 2023). Nepal has an estimated iron ore reserve of approximately 700 million metric tons, primarily derived from two major deposits: the Jhumlabang deposit in Rukum East, estimated at 500 million tons, and the Dhaubadi-Pokhari deposit in Nawalparasi, estimated at 150 million tons. Green ammonia and urea production require hydrogen, nitrogen, and CO_2, which can be sourced from water electrolysis, atmospheric nitrogen, and industrial CO_2 capture respectively, with hydroelectricity powering other complementary processes such as compression and heating (Yapicioglu & Dincer, 2019). The most widely used synthetic method for producing ammonia is the Haber–Bosch Process. In this process, ammonia is produced at a temperature range of 400 °C to 500 °C and pressure in the range of 150–300 bars, usually in the presence of an Iron (Fe) catalyst (Garagounis et al., 2014). Furthermore, ammonia and carbon dioxide (CO_2) are combined under high pressures and elevated temperatures to form ammonium carbamate (NH_2COONH_4), which then decomposes at much lower pressures to yield urea and water (A. Ghimire et al., 2023b). The reaction is also known as the Bazarov reaction. Ammonia can also be transported to the regional market to contribute to the worldwide market size of 156.36 billion USD.

For synthetic fuel production (methane and ammonia), hydrogen, nitrogen, and CO_2 are necessary (Thapa et al., 2024). These can be derived from renewable energy-driven electrolysis, atmospheric nitrogen, and industrial CO_2 capture, respectively. An overview of the resource availability and market demand in 2035 for the use of green hydrogen and renewable electricity in the Nepal Hydrogen Hub is presented in Table 8.3.

The increasing GHG emissions in Nepal are due to the excessive use of petroleum fuels despite the abundance of renewable possibilities in the country. In Nepal, hydropower projects are under various stages of development, and it has started to produce more electricity than consumption during the wet seasons since 2022. A considerable gap in the energy demand and supply scenario is projected in Nepal in the upcoming decade. There is a need for balance between excessive import and use of fossil fuels, spilling of hydroelectricity, and depleting environmental health. In such a scenario, the concept of a Hydrogen Hub can leverage excess hydropower electricity to generate hydrogen and can be used to balance the grid and use it in various industrial applications. The NHH has been proposed and investigated to demonstrate the domestic use of renewable energy for industrial applications.

Table 8.4 presents the estimations of the renewable electricity demand in an optimistic scenario for hydrogen integration in the Nepal Hydrogen Hub in 2035. The results are derived from calculations based on the methodology presented in Table 8.2 and Table 8.3. Table 8.5 presents the summary of the energy consumption scenario in the Nepal Hydrogen Hub for the year 2035. By 2035, Nepal is projected to require 1,857,374 metric tons of diesel, leading to approximately 4.7 million metric tons of CO_2 emissions annually. Battery-powered alternatives are not proven to be unsuitable for heavy-duty vehicles due to

Table 8.3 Resource Availability Summary for Specialized Industrial Zone and Energy Export for 2035 Results and Discussion

S.N.	*Type of Industry/ Applications*	*Proven Resources and Markets*	*Procedures for the application of clean energy*
1	Replace diesel-based Transport	• Nepal has a large hydropower potential that is sufficient to support electrification and hydrogen applications (Bhatt, 2017) • 269388 kL of Diesel Demand (Nepal Oil Corporation, n.d.)	Green Hydrogen as an alternative to Diesel in heavy-duty vehicles
2	Green Ammonia and Green Urea	• Abundant nitrogen in the atmosphere • Industrial CO_2 capture is feasible and commercially available (International Energy Agency, n.d.; Yapicioglu & Dincer, 2019) • 126,400 Metric tons per year of Urea demand in Nepal (Government of Nepal, n.d.)	Hydrogen, Nitrogen, and Carbon dioxide are directly used as feedstock for the production of fertilizer (Allen et al., 2021; Devkota et al., 2023)
3	Replacing Fossil Fuels in Heat-Intensive Applications (Cement, Brick, Boilers, etc.)	• 1.07 billion tons of limestone deposit (Federation of Nepalese Chambers of Commerce & Industry, n.d.) • 151,426 metric tons of coal consumption per year (International Energy Agency, n.d.)	Hydrogen can mainly replace coal in heating-based applications and processes where the need for high-grade heat is high
4	Replacement of LPG for heat Applications	• Viability gap funding for renewable-based projects supported by governments (*AEPC*, 2024) • 107,110 Metric Tons of LPG demand in Nepal. (Nepal Oil Corporation, n.d.)	Hydrogen can be used as a feedstock, and renewable electricity can be used in the heating requirements to produce synthetic fuels
5	Iron ore Reduction(Green Steel)	• H2-DRI technology is under development for commercial use • Nepal has ~500 million metric tons of iron ore deposits (Mahat et al., 2023) • About 418,384 million Metric tons of steel demand yearly (Mahat et al., 2023)	Hydrogen serves as a clean reducing agent for reducing iron ore, replacing carbon-based agents
6	Export of Ammonia to the Regional Market	• 18000 MW of surplus Hydroelectricity (Electricity Regulatory Commission, 2024) • 156.36 billion USD Market Size (Ammonia Market Size & Share Report) • Import needs of neighboring countries like India and China	Green Ammonia is an alternative to the other ammonia produced from carbon-intensive processes

Table 8.4 Renewable Electricity Demand in Optimistic Hydrogen Integration Scenario for 2035

S N	*Industrial Sector under Nepal Hydrogen Hub*	*Product Demand in (10^3 Metric Tons)*	*Total Energy for the Production per Year (10^6 MJ)*	*Hydrogen for Replacement of Fossil Fuels per Year (Tons)*	*Energy for Other Complementary Processes per Year (10^6 MJ)*	*Total Electricity Load for Hydrogen Production Process per Year (10^6 MJ)*	*Displaced Carbon Emission (million tons of CO_2)*
1	Replace diesel-based transport	1857.3	84,510	58,6878	–	84,510	4.7
2	Green ammonia and green urea	0.873 & 800	22,566	157,138	2072.7	22,627.8	2.6
3	Replace coal-based applications(cement, bricks)	1562	35,931	249,520	–	35,931	3.4
4	Replacement of LPG for heat Applications	677	37.23	259	–	37.3	0.01
5	Iron ore reduction(green steel)	2648	29,128	110,333	13,240	15,888	1.5
6	Export of ammonia to the regional market	1500	99,090	255,000	13,500	14,025	4.7

Table 8.5 Overall Energy Consumption Scenario for 2035

Hydrogen demand for Nepal Specialized Industrial Zone	~1,359,130	Tons
Base load electricity demand for hydrogen production	~16,288	MW
Base load electricity demand for axillary processes	~1620	MW
Total demand for electricity for Nepal Hydrogen Hub	~17,908	MW

several limitations. However, Hydrogen Fuel Cell Electric Vehicles (FCEVs) offer a feasible solution, with advantages such as higher energy storage per weight, faster refueling, and higher ranges. Given Nepal's abundant renewable resources, the Nepal Hydrogen Hub prioritizing the adoption of commercial hydrogen vehicles presents a viable pathway for reducing emissions in the transport sector. The 100% replacement of diesel-based transport in Nepal by hydrogen in 2035 demands 586,878 tons of green hydrogen and would displace 4,747,196 tons of CO_2 emissions.

The fertilizer production using green hydrogen and locally available resources has the potential to increase agricultural productivity, reduce food imports, and enhance food security. Nepal's agricultural products come from the arable land of 2,113,700 ha. It has been estimated that Nepal will need 800,000 metric tons of urea fertilizer by 2035. Producing this amount of fertilizer using green hydrogen in the specialized industrial zone can result in the displacement of about 2.5 million metric tons of carbon dioxide emission per year with a direct consumption of 157,138 tons of hydrogen per year. The decarbonization of the existing 124 cement industries in Nepal has been investigated. The replacement of coal with green hydrogen during clinker production in the cement industry could reduce CO_2 emissions by 44–86%, and thus formed green cement could be competitively priced at $80–$150 per ton if electricity costs remained low (Czigler et al., 2020; Jibran & Mahat, 2023). The replacement of coal-based applications in Nepalese industries, including major cement industries in 2035 was projected to require approximately 249,520 tons of hydrogen, displacing around 3.3 million metric tons of CO_2 emissions annually.

The potential of hydrogen-derived synthetic fuels to replace low-heat applications such as LPG in residential heat. It was found that using hydrogen-derived synthetic fuels can displace 677,909 metric tons of petroleum fuels, especially liquified petroleum gas (LPG) imported annually in Nepal. This shift could achieve a reduction of 1911.32 metric tons of CO_2 emissions each year from the direct utilization of 258 tons of hydrogen in heating applications. By 2035, Nepal's steel demand is projected to reach 2,648,000 metric tons. However, Nepal has inactive mines such as the Dhaubadi iron ore deposit, Jhumlabang deposit, Selme Mines, etc. This could be sufficient to fulfill the steel demand in Nepal. Conventional steelmaking processes, which emit 1,800 kg CO_2 per ton of steel, could be replaced with H2-DRI, reducing emissions to 110 kg CO_2 per ton of steel from 1,800 kg CO_2 per ton, thereby replacing 1.4 million metric tons of CO_2 emissions (Carbon-Free Steel Production: Cost Reduction Options and Usage of Existing Gas Infrastructure, n.d.; Mahat et al., 2023, pp. 1–16).

To ensure the feasibility and cost competitiveness of these products and projects compared to conventional fuels-based products, it is essential that necessary policies be introduced. The utilization of otherwise unutilized electricity and the implementation of robust business development strategies could significantly improve the feasibility of such initiatives. The government of Nepal is working on different frameworks to support these projects. Electricity, when provided at a subsidized rate, can enable hydrogen production at a cost as low as $1.17 per kilogram of H_2, thereby substantially enhancing the viability of projects within the Nepal Hydrogen Hub (NHH) (Thapa et al., 2021). For the full-fledged development of the NHH, about 13,772 MW of hydroelectricity will be required. This demand is well within the projected capacity of hydroelectric projects under development in Nepal, where hydropower projects are expected to generate ~20,500 MW by 2030 and are planned to produce 28,500 MW by 2035. The establishment of a Hydrogen Hub holds significant potential not only for decarbonizing Nepal's energy sector but also for optimizing the management of the region's hydroelectricity projects.

The base load electricity requirement for Nepal is expected to reach ~10,200 MW by 2035, leaving a curtailment of approximately 18,000 MW of hydropower development by then. This surplus can be utilized in Hydrogen Hubs to domestically consume in different industries and processes for decarbonization as discussed above. Beyond domestic consumption, surplus electricity from Nepal's hydropower can be strategically utilized to produce green ammonia, which can be exported to neighboring countries to meet their clean energy demands. With a remaining capacity of ≥ 3200 MW to produce 1,500,000 tons of ammonia via the Haber–Bosch Process, Nepal could position itself as a regional leader in sustainable energy by exporting green ammonia to countries like India, Pakistan, and Afghanistan in the west, Tibet and China in the north, and Bangladesh, Myanmar, and Bhutan in the east, as shown in Figure 8.7. This will contribute to the replacement of 4.7 million metric tons of CO_2 emissions. The Nepal Hydrogen Hub as a whole has the prospect of managing hydropower spillage in 2035 and contributing to the replacement of 16.9 million metric tons of CO_2 emissions.

Conclusions and Recommendations

With 99.9% renewable electricity generation and a rapidly growing hydropower installed capacity, Nepal is uniquely positioned to pioneer green hydrogen production. The Nepal Hydrogen Hub represents a promising opportunity for the country to address energy challenges while leveraging its vast renewable energy resources. With its abundant hydropower capacity, Nepal can serve as a strategic center for green hydrogen development, effectively managing spillage while supporting the decarbonization of hard-to-abate sectors such as heavy industry and mass transportation. The Nepal Hydrogen Hub could enable it to increase the domestic consumption of renewable electricity for industrial applications while displacing fossil fuels and creating new jobs. This initiative

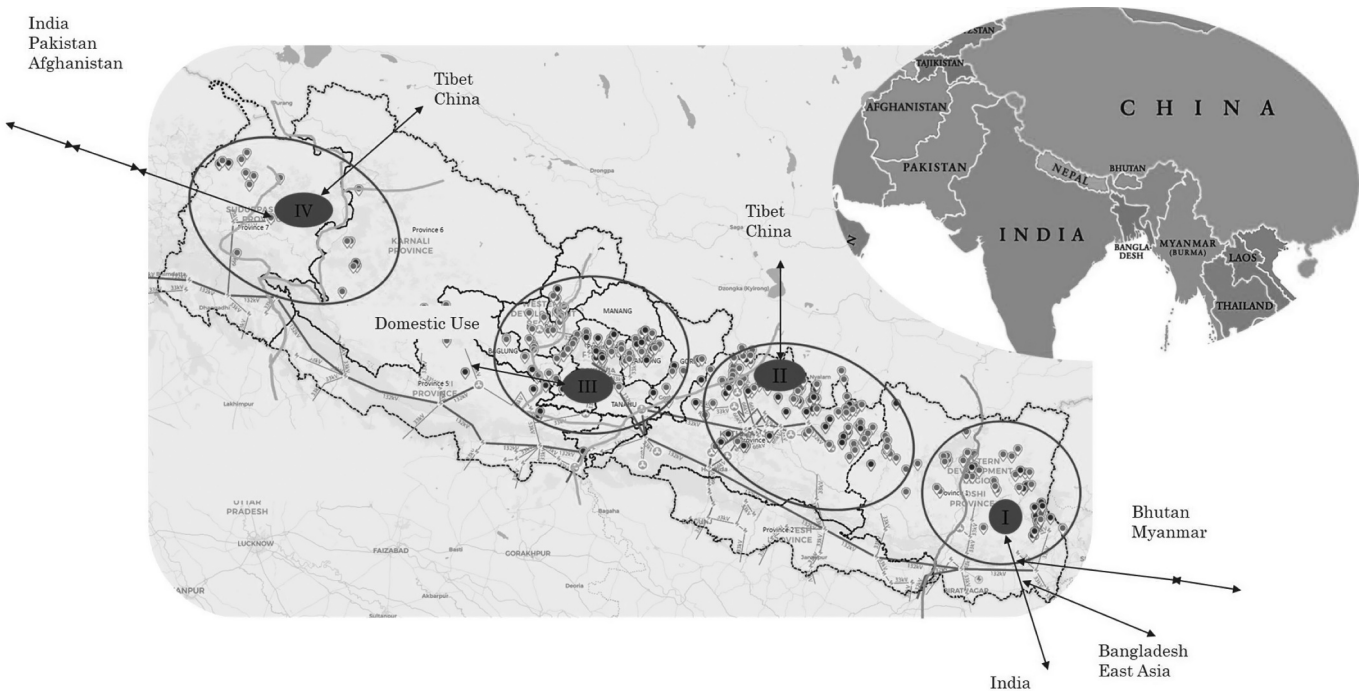

Figure 8.7 Regional market for potential ammonia exports.

not only enhances energy security domestically but also creates opportunities for regional export to South and East Asia, fostering economic growth and contributing to global energy transition goals. Establishing the Nepal Hydrogen Hub will require strategic project planning, strong policy support, and collaborative geopolitical negotiations to attract large-scale investments. By positioning itself as a regional leader in green hydrogen, the Nepal Hydrogen Hub has the potential to drive sustainable energy solutions, promote economic resilience, and solidify Nepal's role as a key player in the global shift toward renewable energy and green growth.

The viability and scalability of the Nepal Hydrogen Hub in Nepal depend upon support from government policies, such as promoting affordable electricity for clean fuel application, the categorization of clean fuels as premium fuels, etc., and, most importantly, on the policy departures for green hydrogen business. Following are the key recommendations identified from this study for further study and to promote pioneering and transformative green energy projects in Nepal Hydrogen Hub:

- A comprehensive study on the techno-economic feasibility and raw materials mapping of individual projects in the Specialized Industrial Zone and the Nepal Hydrogen Hub as a whole is strongly recommended. This study is needed for a clear understanding of the project's overall viability, to identify potential risks, and to support the development of effective strategies for successful implementation.
- The location of the hub is assumed to be ideally based on the concentration of hydropower resources in the region. The modality of the hub is not necessarily to be confined to a single, centralized facility. A more flexible approach can be adopted, with the hub distributed across multiple locations based on the other energy resources and raw material mapping.
- The viability and scalability of large-scale, pioneering projects rely significantly on robust government policies. To foster innovation and attract investments, the government must establish a supportive policy framework that includes tax exemptions, duty reductions, targeted subsidies, and incentives for sustainable projects.
- Blended finance, which combines public and private financial resources, should be recognized as a strategic tool to fund and implement development projects. By leveraging the strengths of both sectors, blended finance can amplify the impact of investments, ensure financial sustainability, and promote shared accountability in high-impact initiatives.
- Innovative project frameworks should be adopted by blending the models such as Public–Private Partnership (PPP), Special Purpose Vehicle (SPV), and Build–Own–Operate–Transfer (BOOT). These frameworks should aim for eventual ownership transfer to the private sector at the project's final stage to ensure long-term sustainability and operational efficiency.
- To enhance the financial attractiveness of green energy businesses, mechanisms that integrate green financing tools with voluntary carbon market

practices should be developed. This approach would enable energy ventures to generate additional revenue streams by trading carbon credits, making green projects more viable while aligning with global climate goals.

Limitations

This study is constrained by the precision and reliability of simulation software and data obtained from the literature. The study primarily concentrates on the concept of the Nepal Hydrogen Hub for better utilization of hydroelectricity and decarbonization of industries in Nepal and does not delve into the specifics of auxiliary components technology and economic aspects of the concept. This study is positioned to serve as a stimulus for further research, contributing to policymakers' and investors' comprehensive understanding of prospects and enabling well-informed decision-making and project development under the guidelines of the National Adaptation Plan 2050. Hydropower is considered the primary energy source due to its vast potential, the study does not account for other renewable sources such as solar and wind, limiting the comprehensiveness of the energy landscape within the Nepal Hydrogen Hub.

Export market assessments are modeled based on potential surplus scenarios rather than actual regional market demands for ammonia, which does not provide accurate export-related scenarios. In terms of environmental impact, CO_2 emissions are evaluated based on direct fossil fuel use, without incorporating a full life cycle assessment (LCA). Furthermore, the study assumes stable economic and policy conditions up to 2035, which may not fully reflect evolving regulations, economic fluctuations, or geopolitical factors that could influence Nepal's green hydrogen market integration and cross-border trade. The energy demand and carbon displacement estimates were calculated as an aggregate for all hubs rather than analyzed individually, potentially masking site-specific challenges or opportunities.

References

AEPC. 2024. Retrieved December24, 2024, from https://www.aepc.gov.np/

Allen, J., Panquet, S., & Bastiani, A. 2021. Electrochemical ammonia: Power to ammonia ratio and balance of plant requirements for two different electrolysis approaches. *Frontiers in Chemical Engineering*, *3*: 765457. https://doi.org/10.3389/fceng.2021.765457

Ammonia Market Size, Share, Analysis, Report, 2032. n.d. Retrieved July18, 2024, from https://www.fortunebusinessinsights.com/industry-reports/ammonia-market-101716

Bhatt, R. P. 2017. Hydropower development in Nepal—climate change, impacts and implications. In *Renewable Hydropower Technologies*. InTech. https://doi.org/10.5772/66253

Carbon emissions from the steel industry|RECCPEDIA|Reccessary. n.d. Retrieved December24, 2024, from https://www.reccessary.com/en/reccpedia/industry/carbon-emissions-from-the-steel-industry

Carbon-free steel production: Cost reduction options and usage of existing gas infrastructure. n.d. https://doi.org/10.2861/01969

Chaudhary, Y., Gautam, S., Poudyal, A., Joshi, R., & Uprety, B. 2022. Review on the different processes of urea production for achieving sustainable development goals in Nepal. *Journal of Institute of Science and Technology*, *27*: 69–81. https://doi.org/10.3126/jist.v27i1.45515

Coke making | industrial efficiency technology & measures. n.d. Retrieved December13, 2024, from https://www.iipinetwork.org/wp-content/Ietd/content/coke-making.html

Czigler, T., Reiter, S., Schulze, P., & Somer, K. 2020. *Laying the foundation for zero-carbon cement*. McKinsey and Company. https://www.mckinsey.com/industries/chemicals/our-insights/laying-the-foundation-for-zero-carbon-cement#/

Department of Electricity Development. n.d. Retrieved December31, 2024, from http://www.doed.gov.np/

Devkota, S., Ban, S., Shrestha, R., & Uprety, B. 2023. Techno-economic analysis of hydropower based green ammonia plant for urea production in Nepal. *International Journal of Hydrogen Energy*, *48*(58): 21933–21945. https://doi.org/10.1016/j.ijhydene.2023.03.087

Electricity generation in India 2023: Share of different sources. n.d. Retrieved July11, 2024, from https://groundreport.in/electricity-generation-in-india-2023-share-of-different-sources/

Electricity Regulatory Commission. 2024. Five-year Roadmap for Electricity Regulatory Commission. In *Electricity Regulatory Commission*, 7–8. Electricity Regulatory Commission.

Energy consumption in Pakistan. n.d. Retrieved July11, 2024, from https://www.worlddata.info/asia/pakistan/energy-consumption.php

Energy consumption in Sri Lanka. n.d. Retrieved July14, 2024, from https://www.worlddata.info/asia/sri-lanka/energy-consumption.php

Energy Institute. 2024. *Statistical Review of World Energy*. https://www.energyinst.org/statistical-review

Energy use in US steel manufacturing. n.d. Retrieved December13, 2024, from http://large.stanford.edu/courses/2016/ph240/martelaro1/

Federation of Nepalese Chambers of Commerce & Industry (FNCCI). n.d. Retrieved December24, 2024, from https://fncci.org/minerals-&-mining--152.html

Fertilizer consumption (kilograms per Hectare of Arable Land)|Data. n.d. Retrieved July18, 2024, from https://data.worldbank.org/indicator/AG.CON.FERT.ZS

Garagounis, I., Kyriakou, V., Skodra, A., Vasileiou, E., & Stoukides, M. 2014. Electrochemical synthesis of ammonia in solid electrolyte cells. *Frontiers in Energy Research*, *2*(January): 75969. https://doi.org/10.3389/fenrg.2014.00001

GHG emissions of all world countries—Publications Office of the EU. n.d. Retrieved December31, 2024, from https://op.europa.eu/en/publication-detail/-/publication/0cde0e23-5057-11ee-9220-01aa75ed71a1/language-en

Ghimire, A., Pandey, B., Ghimire, R., & Thapa, B. S. 2023a. Review of industrial heating and potential low-carbon fuels in the context of Nepal. *Journal of Physics: Conference Series*, *2629*(1). https://doi.org/10.1088/1742-6596/2629/1/012029

Ghimire, A., Pandey, B., Ghimire, R., & Thapa, B. S. 2023b. Review of industrial heating and potential low-carbon fuels in the context of Nepal. *Journal of Physics: Conference Series*, *2629*(1). https://doi.org/10.1088/1742-6596/2629/1/012029

Ghimire, R., Niroula, S., Pandey, B., Subedi, A., & Thapa, B. S. 2024. Techno-economic assessment of fuel cell-based power backup system as an alternative to diesel generators in Nepal: A case study for hospital applications. *International Journal of Hydrogen Energy*, *56*: 289–301. https://doi.org/10.1016/j.ijhydene.2023.12.174

Global Greenhouse Gas Emissions: 1990–2021 and Preliminary 2022 Estimates—Rhodium Group. n.d. Retrieved December28, 2024, from https://rhg.com/research/global-greenhouse-gas-emissions-2022/

Government of Nepal Investment Board: Nepal establishing a fertilizer plant in Nepal: A comparative study and analysis of natural gas vs water electrolysis technology establishing a fertilizer plant in Nepal. n.d.

Government of Nepal Water and Energy Commission Secretariat. 2023a. *Energy Synopsis Report, 2023*.

Government of Nepal Water and Energy Commission Secretariat. 2023b. *Nepal Energy Sector Synopsis Report – 2022*.

Grubler, A., Wilson, C., Bento, N., Boza-Kiss, B., Krey, V., McCollum, D. L., Rao, N. D., Riahi, K., Rogelj, J., De Stercke, S., Cullen, J., Frank, S., Fricko, O., Guo, F., Gidden, M., Havlík, P., Huppmann, D., Kiesewetter, G., Rafaj, P., & Valin, H. 2018. A low energy demand scenario for meeting the 1.5°C target and sustainable development goals without negative emission technologies. *Nature Energy*, *3*(6): 515–527. https://doi.org/10.1038/s41560-018-0172-6

Heath, R., Mulckhuyse, J., & Venkataraman, S. 1985. *The potential for energy efficiency in the fertilizer industry*. 97. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/930741468739305174/The-potential-for-energy-efficiency-in-the-fertilizer-industry

Hosseini, S. E., & Wahid, M. A. 2016. Hydrogen production from renewable and sustainable energy resources: Promising green energy carrier for clean development. *Renewable and Sustainable Energy Reviews*, *57*: 850–866. https://doi.org/10.1016/j.rser.2015.12.112

Hydrogen Valleys. n.d. *Insights into the emerging hydrogen economies around the world – Clean Hydrogen Partnership*. Retrieved December29, 2024, from https://www.clean-hydrogen.europa.eu/media/publications/hydrogen-valleys-insights-emerging-hydrogen-economies-around-world_en

Intergovernmental Panel on Climate Change. 2022. Summary for policymakers. In *Global Warming of 1.5°C*. 1–24. Cambridge University Press. https://doi.org/10.1017/9781009157940.001

International Energy Agency. n.d. *Ammonia technology roadmap towards more sustainable nitrogen fertiliser production*. www.iea.org/t&c/

International Renewable Energy Agency. 2022. *World energy transitions outlook 2022: 1.5°C pathway*. www.irena.org

Khan, R. W. A., & Mumtaz, S. 2018, May 13. *Green and secure energy supply chain: Trough China Pakistan economic corridor*. IACB, ICE, ICTE & ISEC.

Krüger, A., Andersson, J., Grönkvist, S., & Cornell, A. 2020. Integration of water electrolysis for fossil-free steel production. *International Journal of Hydrogen Energy*, *45*(55): 29966–29977. https://doi.org/10.1016/J.IJHYDENE.2020.08.116

Mahat, C., Jibran, J. A., Sharma, N., & Thapa, B. 2023. Challenges and prospects of steel production using green hydrogen in Nepal. *Journal of Physics: Conference Series*, *2629*(1). https://doi.org/10.1088/1742-6596/2629/1/012026

Marahatta, S., Devkota, L. P., & Aryal, D. 2021. Impact of flow variation on hydropower projects in Budhigandaki River Basin of Nepal. *Journal of Institute of Science and Technology*, *26*(1): 89–98. https://doi.org/10.3126/jist.v26i1.37831

Mitra, M., Singha, N. R., & Chattopadhyay, P. K. 2023. Review on renewable energy potential and capacities of South Asian countries influencing sustainable environment: A comparative assessment. *Sustainable Energy Technologies and Assessments*, *57*: 103295. https://doi.org/10.1016/J.SETA.2023.103295

Naveed Iftikhar, M., Najeeb, F., Mohazzam, S., & Khan, S. A. 2015. *Sustainable development policy institute report part title: Energy situation in South Asia report title: Sustainable energy for all in South Asia: Report Subtitle: Potential, challenges, and solutions*.

Nepal Electricity Authority. 2024. *A year in review fiscal year 2023/24*. www.nea.org.np

Nepal Oil Corporation. n.d. *Import and sales*. Retrieved October3, 2023, from https://noc.org.np/import

Overview and key findings – World Energy Investment 2022—Analysis—IEA. n.d. Retrieved July10, 2024, from https://www.iea.org/reports/world-energy-investment-2022/overview-and-key-findings

Pagani, G., Hajimolana, Y., & Acar, C. 2024. Green hydrogen for ammonia production—A case for the Netherlands. *International Journal of Hydrogen Energy*, *52*: 418–432. https://doi.org/10.1016/J.IJHYDENE.2023.06.309

Planning & Development Cooperation Coordination Division, G. of N. M. of A. & L. D. n.d. *Statistical-information-On-Nepalese-Agriculture-2077-78*.

Renewable Energy Agency, I. 2023. *Renewable energy statistics 2023 Statistiques D'énergie Renouvelable 2023 Estadisticas De Energía Renovable 2023 About IRENA*. www.irena.org

Ritchie, H., Rosado, P., & Roser, M. 2023. Per capita, national, historical: how do countries compare on CO2 metrics? *Our World in Data*. https://ourworldindata.org/co2-emissions-metrics

Rouwenhorst, K. H. R., Krzywda, P. M., Benes, N. E., Mul, G., & Lefferts, L. 2020. Ammonia production technologies. *Techno-Economic Challenges of Green Ammonia as an Energy Vector*, 41–83. https://doi.org/10.1016/B978-0-12-820560-0.00004-7

Shahzad, K., & Iqbal Cheema, I. 2024. Low-carbon technologies in automotive industry and decarbonizing transport. *Journal of Power Sources*, *591*. https://doi.org/10.1016/j.jpowsour.2023.233888

Shamim, M. M. H., Silmee, S. M., & Sikder, M. M. 2022. Design and techno-economic analysis of a grid-connected solar photovoltaic system in Bangladesh. In *2022 2nd International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2022*. https://doi.org/10.1109/ICAECT54875.2022.9808078

Thapa, B. S., Neupane, B., Yang, H. Seong, & Lee, Y. H. 2021. Green hydrogen potentials from surplus hydro energy in Nepal. *International Journal of Hydrogen Energy*, *46*(43): 22256–22267. https://doi.org/10.1016/j.ijhydene.2021.04.096

Thapa, B. S., Pandey, B., & Ghimire, R. 2024. Economy of scale for green hydrogen-derived fuel production in Nepal. *Frontiers in Chemistry*, *12*. https://doi.org/10.3389/fchem.2024.1347255

Turton, R. 2012. *Analysis, synthesis, and design of chemical processes*. Prentice Hall.

Typical calorific values of fuels—Forest Research. n.d. Retrieved December13, 2024, from https://www.forestresearch.gov.uk/tools-and-resources/fthr/biomass-energy-resources/reference-biomass/facts-figures/typical-calorific-values-of-fuels/

Water Resources and Energy Sectors. 2013. *Nepal's energy sector vision 2050*.

Yapicioglu, A., & Dincer, I. 2019. A review on clean ammonia as a potential fuel for power generators. *Renewable and Sustainable Energy Reviews*, *103*: 96–108. https://doi.org/10.1016/j.rser.2018.12.023

9 Managing Growth in a Geopolitical Context

India's Energy Diplomacy

Himani Kaushik

Introduction

In contemporary political discourse, energy is acknowledged as a vital element for both advanced and emerging economies, underscoring the significance of energy geopolitics in relation to national security. India, recognized as one of the world's rapidly expanding economies, is witnessing swiftly growing energy demands. Projections indicate that by 2035, India's energy needs will experience substantial increases, with anticipated increases of 183% for natural gas, 121% for oil, and 108% for coal. However, the current energy landscape in India is fraught with challenges. The nation finds it difficult to meet its existing energy consumption, with imports recently accounting for 34.41% of its energy needs, according to World Bank data from 2014. Furthermore, demand is expected to surge by 95% by 2030. Despite possessing considerable reserves of coal and natural gas, domestic energy production has not matched the escalating demand for development, leading to an expected increase in energy imports. Nevertheless, India is committed to an ambitious energy transition aimed at increasing the proportion of renewable energy sources within its energy portfolio. To address these challenges, the country is investigating new energy pathways and tackling environmental concerns associated with conventional energy sources. The importance of energy sources and the guarantee of reliable imports from current resources highlight the essential role of international relations. Consequently, it is not surprising that India's diplomatic initiatives aimed at securing energy resources have gained prominence in recent years. Within the framework of global politics, energy serves as a mechanism for balancing political and economic relationships among countries. Historical trends indicate that nations excelling in this sector possess strategic advantages. As a result, countries have carefully crafted their foreign policies to ensure access to energy resources, thereby broadening their spheres of influence. Additionally, energy resources play a crucial role in forming strategic alliances and fostering partnerships on the global stage. Nation's rich in resources, along with their investment capabilities and technological advancements, have experienced a surge in energy demand and the associated influence. Therefore, the realms of energy diplomacy and geopolitics are intrinsically linked.

DOI: 10.4324/9781003633204-11

India's Energy Diplomacy

India is actively engaging in a proactive strategy of energy diplomacy on a global scale in order to achieve its energy goals. At the same time, the country seeks to navigate the geopolitical landscape effectively, leveraging its energy resources and investments as tools for negotiation. While there is a wealth of research focused on China's energy diplomacy and its consequences, there is a notable deficiency in studies that specifically explore India's energy diplomacy. This chapter aims to investigate the relationship between India's energy-related international relations and the geopolitical dynamics in the South Asian region. To facilitate this exploration, it poses two essential questions: What are the key features of India's energy diplomacy? How does India's energy diplomacy interact with the geopolitical framework of South Asia? To answer these questions, the chapter employs a qualitative methodology, utilizing literature, academic articles, reviews, and secondary sources. Additionally, Myanmar is included in the analysis due to its significant role in South Asian geopolitics and energy supply chains. The chapter is organized into five sections, beginning with an introduction and concluding with a summary of findings. The second section examines conceptual frameworks, while the third evaluates India's energy diplomacy. The subsequent section investigates the connection between India's energy diplomacy and the geopolitical context in South Asia, ultimately leading to a conclusion that synthesizes the overall findings. Countries rich in resources, and equipped with investment and technological capabilities, have experienced a rise in energy demand and the accompanying influence. Consequently, the domains of energy diplomacy and geopolitics are inherently interconnected.

Energy considerations are pivotal to the discourse surrounding international relations (IR). Historically, coal has been instrumental in influencing global interactions, particularly during the 18th and 19th centuries. The concept of transnational energy relations is intricately linked to energy security, as underscored by the Asia Pacific Energy Research Centre (2007), which asserts that the security of energy supply is contingent upon a variety of factors, including geopolitical dynamics, resource availability, energy pricing, and environmental sustainability. Energy has been a persistently fundamental element of the global political economy. In contemporary political dialogues, energy is acknowledged as a vital concern for both developed and developing nations, highlighting the significance of energy geopolitics in relation to national security. India, which is recognized as one of the fastest-growing economies worldwide, is confronted with rapidly increasing energy demand. Despite possessing considerable reserves of coal and natural gas, domestic production remains inadequate.

Energy production has faced challenges in keeping pace with the swiftly growing demand for development, leading to an anticipated increase in energy imports. Nevertheless, India is committed to an ambitious energy transition aimed at increasing the proportion of renewable energy sources within its

overall energy portfolio. To effectively address these challenges—such as exploring new energy pathways, tackling environmental concerns associated with conventional energy sources, and ensuring reliable imports from current resources—international relations play a crucial role. Thus, it is not surprising that India's diplomatic initiatives to secure energy resources have gained prominence in recent years. In the realm of global politics, energy serves as a critical instrument for managing the political and economic ties between nations. Historical trends indicate that countries possessing energy resources often enjoy significant strategic advantages. Consequently, the foreign policies of these nations are frequently designed to guarantee energy supply security, thereby expanding their spheres of influence. Furthermore, energy resources are vital for forming strategic alliances and fostering partnerships on the international front. The recent involvement of China, India, and other emerging economies in the global energy landscape has notably altered the existing dynamics. South Asia, in close proximity to India, has emerged as a crucial arena for energy competition. The region's untapped energy potential and strategic location have attracted the interest of various local and regional actors in energy politics. Resource-rich nations, bolstered by investments and technological advancements, have experienced a surge in energy demand and the accompanying influence. As a result, the domains of energy diplomacy and geopolitics are closely intertwined.

India is poised to adopt a proactive approach in its global energy diplomacy to fulfill its energy objectives. Concurrently, it aims to adeptly navigate the geopolitical terrain, utilizing its energy resources and investments as tools for negotiation. While there has been considerable scholarship on China's energy diplomacy and its implications, there remains a significant gap in research concerning India's energy diplomacy. This chapter endeavors to explore the connections between India's energy-related international relations and the geopolitical dynamics within South Asia. To guide this inquiry, the chapter poses several critical questions around the changing nature and role of energy diplomacy and India's interaction within the South Asian landscape. To address these inquiries, the chapter employs a qualitative methodology, drawing on literature, academic publications, reviews, and secondary sources. Additionally, Myanmar is incorporated into various discussions due to its significant role in South Asian geopolitics and energy supply chains. The chapter is divided into five sections, including an introduction and conclusion. The second section delves into conceptual issues, while the third evaluates India's energy diplomacy. The subsequent section investigates the relationship between India's energy diplomacy and the geopolitical context in South Asia, leading to the final section, which concludes the discussion.

Conceptual Frameworks in Energy Diplomacy

Mariët Druif (2019) highlights that energy diplomacy serves not only to secure access to energy resources but also to foster sustainable energy production and

consumption. Nevertheless, many definitions of energy diplomacy primarily focus on state actors, often neglecting the roles of other stakeholders within the energy market. The study of international energy relations is inherently multidisciplinary. The objectives of energy diplomacy can vary significantly for energy-rich nations like the United States, where the focus is on leveraging energy to further strategic interests internationally. Achieving access to energy resources may necessitate the use of threats, economic sanctions, or military intervention, illustrating the application of hard power. Pascual (2015) has demonstrated the impact of hard power strategies on energy markets through his 'rules of Six' framework, which he applies to various nations and regions. In contrast, Griffiths (2011) posits that while nations rich in resources may achieve success through coercive or compensatory hard power strategies, most countries lack the requisite physical or financial means to adopt a hard power stance in their energy policies. As a result, both Griffith and Druif agree that the attainment of energy objectives requires an emphasis on collaboration rather than coercive tactics.

Furthermore, energy diplomacy is viewed as a manifestation of soft power, where the effectiveness of diplomatic initiatives in advancing a nation's energy interests hinges on the influence it can wield over its allies. Within the realm of international relations, the United States is noted for its preference for more coercive approaches, while the European Union (EU) generally advocates for a multilateral, incentive-driven strategy to address energy security issues, likely reflecting its constrained military capabilities and collective approach. In theoretical discussions, Reinhardt and Pronichkin (2015) argue that the realist framework of global relations offers the most lucid insight into modern energy diplomacy. The realist paradigm asserts that states are the primary entities in international energy relations, motivated chiefly by the necessity of self-preservation in a disordered system devoid of a central authority.

Although realists acknowledge the increasing role of global institutions and diverse political actors, they contend that multinational corporations function within a context shaped by both formal regulations and informal influences. Conversely, Simon Xu Hui Shen (2015) critiques the realist viewpoint for inadequately addressing the intricacies of energy diplomacy, despite the efforts of states to enhance their energy security. He argues that in the contemporary global environment, the extraction of foreign energy resources without a grounding in values or ideology may violate modern norms related to peace and sustainability, potentially leading to repercussions, both domestically and internationally. Consequently, states frequently incorporate qualitative dimensions into their resource strategies, framing these actions in terms of values or ideologies to portray them as less self-serving. To clarify this concept, Simon introduces the notion of 'Qualitative Energy Diplomacy (QED),' which, he asserts, is consistent with the constructivist perspective in International Relations.

This viewpoint situates energy initiatives within various ideological contexts, prompting ethical evaluations of non-cooperative states by others. While the approaches adopted by different nations concerning QED may vary, it is

generally noted that countries exhibiting greater internal diversity are more inclined to emphasize their values in diplomatic interactions. Geopolitics, which investigates the relationship between geographical factors and global political dynamics, has historically concentrated on national conflicts over territorial claims and the military tactics employed to gain strategic advantages. Over the years, however, this discipline has expanded to address a broader spectrum of issues, increasingly underscoring the role of geographical elements in shaping state power. In a similar vein, the field of international relations has progressed to highlight the significance of natural resources, their geographical distribution, transportation networks, and critical chokepoints. Given the scarcity of energy resources, securing energy under advantageous conditions is crucial and can significantly influence the interactions among competing consumer nations. Scholars within the field of International Relations have devoted substantial attention to the strategies that states employ to guarantee energy security, particularly through resource accumulation and the management of essential transportation routes. The exploration of the nexus between geopolitics and energy can be traced back to the 1970s and 1980s. In a foundational study on energy geopolitics, Conant and Gold (1980) posited that geographical factors and state-level decisions play a critical role in the ability to secure energy resources.

A multitude of researchers have employed geopolitics as a theoretical lens to analyze energy politics and the safeguarding of energy supplies. Ian Skeet (1996) described the geopolitics of energy as the 'influence of resource locations on the political dynamics of states.' Furthermore, Ioannis Vidakis and Georgis Baltos introduced the term 'geoenergia' to elucidate the impact of energy resources on political and economic systems, as well as on international relations. The field of energy geopolitics aims to explore the connections between geopolitical assessments and energy-related issues.

Discussions on energy geopolitics underscore the intricate interdependence between energy consumers and producers. This relationship is characterized by its dynamic nature, which carries substantial implications. Technological innovations are reshaping the demand for raw materials, thereby affecting both international and domestic policy frameworks. The evolving global landscape is a direct consequence of these technological advancements. Numerous countries continue to depend on energy resources, a central theme in the discourse on energy geopolitics. A comprehensive examination of energy exploration, transportation, development, and the demand–supply chain is essential for a nuanced understanding of international energy frameworks and the complexities of energy systems across different nations. Historically, this concept has deepened the comprehension of energy frameworks and their dynamic interactions. The conventional perspective on energy geopolitics primarily focuses on the supply routes for fossil fuels. Nations endowed with energy resources have sustained a competitive edge in various critical sectors. For example, the United States, as a prominent energy producer, has leveraged its energy resources to fulfil its global energy objectives. In the contemporary context, Russia's

preeminence in the European gas market significantly bolsters its influence in global political affairs. A distinct rivalry among major powers is apparent as they compete for control over vital energy transit chokepoints, such as the Strait of Hormuz. Protecting natural gas pipelines is crucial for the operational stability of energy geopolitics. The dialogue surrounding the growth of emerging economies, particularly China and India, emphasizes their varied energy needs. Many experts evaluate the management and utilization of natural resources and the wealth generated by developing nations, often highlighting the disproportionate advantages enjoyed by more developed economies.

As the awareness of the ramifications of climate change intensifies, the discourse surrounding energy geopolitics has become increasingly complex. There is a growing collective demand and international pressure for nations to diminish their dependence on fossil fuels. Consequently, new dimensions of energy geopolitics are emerging in the contemporary context. While countries strive to safeguard their hydrocarbon resources, they are simultaneously undertaking initiatives to evaluate and mitigate their carbon emissions. Within this framework, economies are adopting a variety of strategies to lessen their carbon footprints and investigate alternatives to conventional fossil fuels.

Geopolitical Dynamics of India's Energy Diplomacy

A rising number of nations are proactively pursuing clean energy options. This chapter broadly characterizes energy diplomacy as a strategic tool of foreign policy designed to advance national interests related to energy security. These interests may include the procurement of energy resources from other countries, the formation of sustainable energy alliances, or the negotiation of favorable agreements to achieve national objectives. The analysis adopts a state-centric perspective, concentrating on India as a key player, rather than delving into the various organizations within the country that participate in the energy sector. The relationship between energy diplomacy and geopolitics is complex, with each domain exerting influence over the other. This study will examine the geopolitical ramifications of both fossil fuels and renewable energy, extending beyond mere discussions of energy transition and geopolitics. Historically, energy has been a pivotal element in a nation's foreign policy; however, the notion of energy diplomacy has only recently garnered significant attention.

This section will investigate the historical context, goals, initiatives, and theoretical foundations of India's energy diplomacy. The significance of international energy collaboration, whether through bilateral or multilateral agreements, has always been crucial for India. The Indian government is also prepared to further explore these avenues. In partnership with the Ministry of External Affairs, the Ministry of Petroleum and Natural Gas (MoPNG) and the Ministry of New and Renewable Energy engage with various governments and organizations to create Memoranda of Understanding aimed at enhancing collaboration in their respective sectors.

In September 2007, the Ministry of External Affairs initiated an energy security division, which was later merged with the Investment and Technology Promotion (ITP) division. This division is responsible for working alongside relevant ministries to strengthen their international initiatives through suitable diplomatic measures, including the establishment of partnerships with energy-related enterprises, forums, and think-tanks. Since its independence in 1947, India's energy policy has primarily focused on addressing the growing energy needs. However, the strategies employed to tackle this challenge have profoundly influenced both the formulation of Indian energy policy and its energy diplomacy. Historically, India's national policy has emphasized self-sufficiency since independence, leading to a persistent emphasis on coal-based energy resources. The Indian government has implemented numerous initiatives to enhance supply and regulate domestic energy consumption, although not all have achieved the desired outcomes.

The recent shift in energy policy underscores the increasing importance of alternative energy sources. As the domestic output of oil, gas, and coal continues to diminish, India is becoming more aware of the potential aggravation of its energy crisis. This awareness has bolstered the argument that enhancing energy security in India can be effectively achieved through the acquisition of oil, gas, and coal from global markets. Such imports are expected to provide supply security and price stability, while also addressing ongoing challenges related to India's balance of payments. By expanding its international engagement, India seeks to diversify its energy portfolio and enhance its competitiveness on the global stage by developing expertise within the energy sector. Despite encountering supply disruptions and a growing trade deficit, India has persistently increased its energy imports. This approach has been further driven by China's intensified efforts to secure external resources. Currently, India's energy diplomacy embodies a blend of strategies aimed at forming partnerships, acquiring resources, and obtaining advanced technologies. The Indian government is actively promoting domestic companies to invest in foreign oil and gas assets and to engage in international exploration and production initiatives. At present, India holds offshore oil and gas projects and assets in 26 countries, with ambitions to significantly increase this number. The country has consistently sought participation in international natural gas pipeline projects, including the Iran–Pakistan–India pipeline, the Turkmenistan–Afghanistan–Pakistan–India Pipeline (TAPI), and the Myanmar–Bangladesh–India pipeline.

Additionally, India aims to expand its portfolio of liquefied natural gas (LNG) contracts while leveraging diplomatic channels to secure a more substantial supply from key suppliers, particularly Saudi Arabia and the UAE. Additionally, there is an increasing emphasis on bolstering India's domestic energy capacity and market.

The government is actively investigating the influence of foreign policy on the persistent inequalities within India's energy sector. A significant development in this context is India's transition from the Japan Crude Cocktail (JCC) pricing model for natural gas imports to the Henry Hub pricing model, which

is perceived as more economically advantageous. Furthermore, India's energy diplomacy is strategically aligning itself with a future that prioritizes alternatives to fossil fuels, consistent with the comprehensive energy transition strategy outlined by the Modi administration. The prime minister has underscored the importance of utilizing foreign policy to obtain increased support, subsidized loans, and a variety of international investments and technologies in the energy sector. During the prime minister's official visits to Japan and the United States, joint statements prominently addressed issues such as investment, technological collaboration, and financial support for solar energy initiatives. In April 2021, Prime Minister Modi and President Joseph Biden formalized the 'India–US Climate and Clean Energy Agenda 2030 Partnership,' which underscores the urgent need to mobilize resources for the rapid implementation of clean energy solutions and the development of innovative technologies. The electoral agenda of the Bharatiya Janata Party (BJP) has emphasized the importance of advancing the strategic nuclear energy program. Consequently, the enhancement of India's nuclear energy capabilities has become a pivotal aspect of Narendra Modi's foreign policy. Recent data indicates that India has established civil nuclear agreements with 14 countries and it stands out as the only nation outside the Nuclear Non-Proliferation Treaty (NPT) permitted to engage in nuclear material trade (Table 9.1).

India's growing energy demands, coupled with its progress in renewable energy technologies, have positioned the country as a significant player in the global energy arena. This strategic advantage is being leveraged by India to bolster its status as an emerging energy leader internationally. Moreover, India has taken a more assertive approach, exemplified by its hosting of the 16th International Energy Forum Ministerial, April 10–12, 2018. In parallel, the United States has pledged to host the ninth Asian Ministerial Energy Roundtable of the International Energy Forum (IEF) in 2022. Through its Ministry of New and Renewable Energy, India has been offering specialized training programs in solar and wind technologies to African and other developing nations. These initiatives highlight India's commitment to leveraging its clean energy expertise to forge partnerships with various countries. The nation's strategy for acquiring energy assets and oil resources can be characterized as both 'mercantile' and 'pragmatic.' India is actively engaging in diplomatic efforts to strengthen bilateral ties with energy-rich nations. Countries such as Venezuela and Iran, which are currently under US sanctions, serve as significant energy suppliers for India. The sanctions on Iran have prompted India to reevaluate its limited options for sourcing energy from the United States. A similar dynamic is evident in India's relationship with Russia, especially in the context of the ongoing conflict in Ukraine. Furthermore, India has effectively utilized its robust connections in the Middle East to secure oil imports from traditional suppliers, including Saudi Arabia, Kuwait, and the UAE.

Considering apprehensions surrounding possible disruptions in the supply of natural gas and oil, alongside persistent geopolitical tensions and price

Table 9.1 Major India-Financed Projects for Energy Cooperation in South Asia (2005–2023)

Country	*Project*	*Indian Project Finance (in US $ Million)*
Bangladesh	India Bangladesh friendship pipeline	35
Bangladesh	Maitree 1320MW super thermal power plant	1600
Bangladesh	SASEC 1000MW-HVDC Bangladesh India electrical grid interconnection project I	98
Bangladesh	SASEC 500MW-HVDC Bangladesh India electrical grid interconnection project II	120
Bangladesh	Kathiar–Parbotipur– Bornagar 1220MW-HVDC double circuit cross-border line	283
Bhutan	Tala 1020MW Hydel Power Plant	89
Bhutan	Chukha 556MW Hydel Power Plant	48
Bhutan	Kurichu 36 MW Hydel Power Plant	19
Bhutan	Dorjilung 1125MW Hydel Power Plant	400
Bhutan	1200MW Punatsangchu I,1020 MW Punatsangchu II Hydel Power Plant	386
Bhutan	600MW Kholongchu Hydel Power Plant	228
Bhutan	720 MW Mangdechhu Hydel Power Plant	586
Nepal	Motohari–Amblekhgunj Petroleum pipeline	2.8
Nepal	Sapta Kosi high dam project and Sun Koshi storage cum diversion	N/A
Nepal	Arun-3 Hydroelectric project	983
Nepal	Upper Karnali Hydroelectric project	975
Nepal	Rahughat Hydroelectric project	67
Nepal	Pokhra 1MW Hydel Power Plant	5.29
Nepal	Trisuli 21 MW Hydel Power Plant	17.7
Nepal	Devighat 14.1 MW Hydel Power Plant	8.23
Sri Lanka	India-Sri Lanka undersea transmission line	1200
Total number of countries: 4	Total no. of energy cooperation projects: 22	Total amount: US$ 7.15 billion

Source: The Ministry of Energy, GoI, the Ministry of External Affairs, GoI

fluctuations, the Indian government has adopted a forward-looking diversification strategy. Remarkably, while maintaining strong relations with the United States, India has effectively continued its productive partnership with Russia in the energy sector. The initiative to import liquefied natural gas (LNG) has not only broadened India's array of gas-exporting allies but also attracted a significant investment of $13 billion from a Russian firm for the establishment of a 20-million-ton refinery and a network of fuel stations. Furthermore, India has been collaborating with Russia on various nuclear projects. The country is also receptive to forming partnerships with China to bolster its energy landscape. In recent years, India and China have tentatively agreed to create a consumer coalition aimed at jointly negotiating oil resources, thereby establishing a collaborative working group focused on energy matters. These developments unfold against the backdrop of increasing US sanctions on Iran

and Venezuela, which are anticipated to reduce the sway of OPEC nations, particularly Saudi Arabia, the primary oil supplier to both countries, over global oil pricing.

Additionally, both India and China are eager to include Japan and South Korea in this coalition, as they rank as the second- and fourth-largest energy importers globally, respectively. Analysts suggest that India's foreign policy embodies a pragmatic realist perspective globally, indicating a shift towards realist nationalism Madan, 2020). Former Indian President A. P. J. Abdul Kalam articulated that his efforts to enhance India's nuclear capabilities were aimed "to assure the several million masses of India, to never feel small or powerless." This perspective also shapes India's foreign policy concerning energy matters. The nation's ambition to position itself as a significant player in the energy arena and its quest for self-sufficiency are fundamental aspects of its energy strategy. Nevertheless, a qualitative approach to energy diplomacy is crucial for elucidating India's international relations in this sphere.

Major Energy Projects in South Asia

India's energy diplomacy is primarily grounded in practical considerations, yet it is also driven by a nationalistic conviction that emphasizes the importance of achieving its objectives within the context of global political dynamics. This strategy involves leveraging diplomatic channels to secure energy resources, enhance energy security, and access technologies that align with its strategic interests. Consequently, the essence of India's energy diplomacy lies in its ability to adapt to evolving circumstances: it encompasses both the importation and exportation of energy resources and technologies while adeptly navigating competition and collaboration with various stakeholders as necessary. India's strategic geographical position presents considerable advantages for the United States concerning cross-border energy and power transactions. The country is actively engaged in energy connectivity initiatives with nearly all its South Asian neighbors, including Bhutan, Nepal, and Bangladesh. Currently, Bhutan provides India with between 1,000 and 1,200 MW of energy. Moreover, two 400kV D/C (quad) cross-border interconnection lines are under construction, which, upon completion, will elevate the total transfer capacity between the two nations to 4,250 MW. Additionally, India and Nepal are working together on a significant energy exchange project in South Asia, characterized by cross-border energy collaboration.

The estimated transmission capacity is approximately 1,500 MW. India and the Maldives have formalized their partnership in energy efficiency and renewable energy through a Memorandum of Understanding (MoU). In the context of the ongoing energy transition, India's proactive measures in the renewable energy sector have positioned it as a crucial ally for countries in South Asia. For instance, since 2013, India has been supplying energy to Bangladesh, with the provision increasing to 1,160 MW. In return, Bangladesh has permitted India to use its transit facilities and grid to facilitate energy distribution to

India's Northeast region. In 2011, Bangladesh entered an MoU with the Indian Ministry of New and Renewable Energy to enhance technical cooperation in renewable energy initiatives. Furthermore, the 2018 tripartite agreement involving India, Russia, and Bangladesh to collaborate on the Rooppur Nuclear Power Plant represented a significant advancement in recognizing India's nuclear capabilities on the international stage. Within the energy landscape of South Asia, India remains particularly attentive to the growing influence resulting from China's ascent.

The primary objective of energy diplomacy is to secure access to vital resources and ensure reliable transportation routes. Geopolitical strategies necessitate the development of influence over neighboring countries through strengthened energy sector partnerships. Given the limited availability of easily accessible energy resources in South Asia, there has been a notable shift towards promoting investment and collaboration in this area to enhance regional influence. Many South Asian countries are collaborating with both India and China on their energy projects. As a result, two primary areas of focus have emerged: investment in the energy sector and the advancement of renewable energy sources. During this transformative era for energy, both India and China have positioned themselves as crucial players. China is striving to take the lead in clean technology, thereby presenting itself as an attractive partner for South Asian countries seeking sustainable energy alternatives. Chinese companies are heavily involved in the establishment of hydroelectric and renewable energy initiatives across various South Asian nations, including Pakistan, Bangladesh, and India.

India's Transition Towards Renewable Energy

India's escalating energy demands, alongside significant advancements in renewable energy technologies, have positioned the nation as a key player in the global energy landscape. This emerging status is being strategically harnessed by India to bolster its role as an influential energy actor internationally. In 2022, the United States pledged to host the ninth Asian Ministerial Energy Roundtable, facilitated by the International Energy Forum (IEF). Through its Ministry of New and Renewable Energy, India has initiated training programs targeting African and other developing nations, with a focus on the wind and solar sectors. These initiatives enable India to capitalize on its clean energy knowledge while fostering collaborations with various countries. India's strategy for securing petroleum resources and energy supplies is characterized by a 'commercial' and 'pragmatic' approach. The country utilizes political tools to strengthen bilateral ties with energy-abundant nations and has demonstrated a willingness to engage with countries often regarded as pariahs, even by its closest allies. This is particularly evident in its interactions with nations like Venezuela and Iran, which, despite facing US sanctions, remain vital energy providers for India. The sanctions imposed on Iran have been viewed as a strategic advantage for India, given the limited options for sourcing energy from

countries aligned with US interests. A similar dynamic can be observed in India's relations with Russia in the context of the Ukraine crisis.

India has adeptly utilized its robust connections in the Middle East to secure oil imports from historically reliable suppliers, including Saudi Arabia, Kuwait, and the UAE. Considering apprehensions surrounding possible interruptions in natural gas and oil supplies, persistent geopolitical instabilities, and price volatility, the Indian government has taken proactive measures by adopting a diversification strategy. Importantly, while maintaining a strong partnership with the United States, India has also managed to sustain positive relations with Russia in the energy domain. The initiative to import liquefied natural gas (LNG) has not only broadened India's array of gas-exporting partners but also attracted a substantial investment of $13 billion from a Russian firm aimed at developing a 20-million-ton refinery along with a network of fuel stations. Furthermore, India is actively engaging in collaborative efforts with Russia on nuclear energy initiatives and is open to forming partnerships with China to bolster its energy infrastructure.

Recent developments indicate that India and China have put forth a proposal to create a consumer coalition aimed at negotiating oil resources collectively. This initiative seeks to establish a collaborative working group dedicated to addressing energy-related issues. The backdrop of this proposal is characterized by escalating US sanctions on Iran and Venezuela, which are anticipated to reduce the influence of OPEC nations, particularly Saudi Arabia—the largest oil exporter to both India and China—on global oil pricing. Additionally, both countries are keen to involve Japan and South Korea in this coalition, as they rank as the second- and fourth-largest energy importers globally, respectively. Analysts suggest that India's foreign policy is rooted in a Realist interpretation of international relations, reflecting a shift towards realist nationalism.

Former Indian President A. P. J. Abdul Kalam articulated that his initiatives to enhance India's nuclear capabilities were intended "to assure the several million masses of India, to never feel insignificant or powerless." This perspective encapsulates India's foreign policy approach concerning energy issues. The nation's ambition to position itself as a significant player in the energy sector, coupled with its quest for self-sufficiency, are pivotal elements of its energy diplomacy. However, the qualitative dimensions of this diplomacy are essential for understanding India's international relations in this field. While fundamentally guided by realist principles, India's energy diplomacy is also bolstered by a nationalist framework that drives it to fulfill its goals on the global stage. This includes the strategic application of diplomacy to secure energy resources, acquire necessary technologies, and advance its interests.

Thus, the essence of India's energy diplomacy lies in its capacity to adapt to changing circumstances, effectively balancing the import and export of energy resources and technologies while managing competition and collaboration with various stakeholders as appropriate. A notable instance of competitive dynamics in the energy sector is evident in Sri Lanka, where a Chinese firm secured a contract for solar and wind energy projects along the Tamil Nadu

coastline in India, prompting significant protests from the Indian government. Furthermore, various state-owned Chinese companies have established a formidable presence in the renewable energy infrastructure across South Asian nations, including Pakistan and Bangladesh. Since 2014, China has invested in a cumulative total of 12,622 MW in solar and wind energy initiatives throughout South and Southeast Asia.

The geopolitical rivalry in the energy domain is particularly illustrated by the situation in Nepal, which is strategically located between India and China. Historically, since achieving autonomy in 1923, Nepal has fostered close ties with India, its southern neighbor. The two countries have been vital partners in energy cooperation within South Asia, with Nepal primarily exporting its hydroelectric power to India. Concurrently, Nepal has sought to establish significant energy collaborations with China, which has emerged as a key investor in the current global landscape. As China sought to enhance its influence in Nepal, India expressed apprehensions regarding these developments. Reports suggest that Nepal and China have opted to halt the 750-megawatt West Seti hydroelectric project due to uncertainties related to the feasibility of electricity exports to India. The absence of access to the Indian market, the main consumer of Nepal's energy, has led to a decline in interest from Chinese companies in this project. Despite the cessation of this initiative, China's investments in Nepal's energy sector continue to be substantial. Both countries have signed MoUs to strengthen energy cooperation, targeting various areas such as hydropower, wind energy, solar power, biomass energy, and other renewable sources, along with grid infrastructure development. Conversely, India is also amplifying its energy diplomacy in Nepal. In 2022, Nepal and India formalized an agreement to launch new hydroelectric projects that would be jointly financed by both nations. Furthermore, India pledged to increase its electricity imports from Nepal and formed a joint venture with the Nepalese government.

These initiatives by India can be interpreted as a countermeasure to China's influence. Through its foreign policy, India has fostered a cooperative relationship with neighboring countries to maintain a regional framework that protects its strategic interests. However, India's involvement in South Asia's energy sector has yet to reach its full potential. Efforts to establish an ambitious regional energy grid across South Asia have progressed slowly. Given its strategic position, India wields considerable influence in facilitating regional energy collaboration, as all South Asian nations can connect through its territory. Nonetheless, India's preference for bilateral agreements and hesitance to pursue multilateral projects have led to dissatisfaction among its neighbors.

China's significant investments in both conventional and renewable energy sectors offer a considerable opportunity for South Asian countries aiming for swift development. In this context, India and China emerge as potential partners in the energy field. Various nations are actively collaborating with both countries on multiple initiatives. To sustain strong ties with its neighbors and counterbalance China's growing influence in South Asia's energy landscape,

India must enhance its energy diplomacy to cater to the specific requirements of its neighboring states. India should engage more intentionally with regional allies through frameworks such as the Bangladesh, Bhutan, India, Nepal (BBIN) initiative and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC). The 'neighborhood first' policy is a fundamental aspect of the Modi administration's diplomatic approach. However, for this strategy to be effective, India must reinforce its position as a regional leader dedicated to fostering mutual benefits. It should aim to be a leader that not only protects its own interests but also champions the collective progress of the region. Recent discussions have focused on enabling energy exports from Nepal via Indian pipelines, and an MoU has been established between Nepal and Bangladesh to facilitate power exchange through the Indian transmission network. These developments are anticipated to enhance India's standing on the global stage. India should capitalize on the evolving geopolitical dynamics linked to energy transition to further its initiatives in hydroelectric power and other renewable energy domains. The nation's ambitious initiative, 'One Sun, One World, One Grid,' seeks to establish a unified solar energy distribution network connecting 140 countries, which could yield considerable benefits for its South Asian neighbors.

Concurrently, India could solidify its position as a leader in renewable energy by intensifying diplomatic efforts aimed at developing regulatory frameworks for technological standardization, thus fostering a more equitable environment for green technology enterprises. Failing to pursue this initiative may hinder India's ability to counteract China's expanding influence in South Asia, which has been bolstered by affordable renewable energy technologies and substantial investments.

Conclusion

Energy is a crucial element in the economic development and prosperity of a nation. As a rapidly growing economy, India encounters significant challenges in managing its swift transformation. The energy collaborations that India establishes with its South Asian neighbors are integral to its foreign policy and energy security framework. By investing in regional energy infrastructure and promoting interdependence, India aims to stimulate economic growth, mitigate China's influence, and enhance its global position. Although geopolitical tensions and varying agendas present ongoing challenges, the advantages of energy cooperation are evident. As India continues to progress on the global stage, its energy diplomacy is anticipated to play an increasingly influential role in shaping the region's future. The structure of India's energy policy should be crafted to reflect the dynamic interactions between domestic and international elements. At its core, India's energy diplomacy is centered on securing energy supplies, diversifying energy sources, and negotiating advantageous terms to tackle domestic energy issues. This strategy underscores a multifaceted approach aimed at ensuring international energy access while attracting investments and securing cost-effective resources.

To enhance its long-term energy independence, India is proactively establishing bilateral partnerships with nations rich in energy resources and is willing to collaborate with competitors to fulfill its energy objectives. As a result, Indian energy diplomacy is marked by a desire to exert substantial influence within the realm of global energy politics. This analysis argues that the concept of QED is crucial for understanding India's motivations in its energy pursuits, particularly in relation to its competition with China. The quest for energy resources and the imperative of securing transportation routes are closely intertwined with geopolitical tensions and conflicts. In the context of South Asia, India's energy strategy is multifaceted. The region demonstrates a dual approach to energy management. On one hand, there is a focus on harnessing local energy reserves and ensuring supply from domestic sources. Conversely, there is a strong emphasis on fostering collaborative initiatives within the energy sector to enhance relationships with neighboring countries. Additionally, the presence of numerous developing economies in the region positions it as a burgeoning market for innovative and renewable energy solutions. India is in competition with China in the South Asian energy landscape, with China's strong ties to Pakistan amplifying India's concerns regarding energy access in the western part of South Asia. Many countries in the region are actively pursuing energy partnerships with both India and China, while India faces challenges arising from China's substantial investments in the area. Thus far, India has maintained a Realist approach in its energy diplomacy, which has hindered several cross-border energy projects.

To strengthen its presence in South Asia, India should adopt a more assertive approach to its energy diplomacy. By sincerely taking on the responsibilities of a regional leader and striving for the collective advancement of South Asia, India can achieve significant advantages. Its advantageous geographical location within the region provides India with a distinctive opportunity to foster local energy collaboration, which can be strategically leveraged to counterbalance China's influence in this domain. Ultimately, India's efforts in regional energy cooperation necessitate a thoughtful and strategic navigation of a complex set of economic, technical, and geopolitical obstacles. This deliberate strategy is essential for ensuring that India not only benefits from enhanced energy partnerships but also positions itself as a trustworthy and competent partner in the shifting dynamics of global energy initiatives.

Bibliography

Amin, A. Z. 2017, November. *The age of renewable energy diplomacy, EDA reflection*. Emirates Diplomacy Academy. Retrieved from https://eda.ac.ae/docs/default-source/Publications/eda_reflection_age_of_renewable_energy_en.pdf?sfvrsn=2

Asia Pacific Energy Research Centre. 2007. *A quest for energy security in the 21st century: Resources and constraints*. Japan: Institute of Energy Economics.

Bandyopadhyay, A. 2016, May 8. *Energy diplomacy to secure India's energy future*. Financial Chronicle.

Boersma, T., & Johnson, C. n.d. *US energy diplomacy*. New York: Center on Global Energy Policy, Columbia University.

Campbell, C. 2019, November 1. *China is bankrolling green energy projects around the world*. Time.

Chaudhuri, P. P. 2015, March 13. *Fragmented and fitful: India's energy diplomacy*. Rhodium Group. Retrieved from https://rhg.com/research/fragmented-and-fitful-indias-energy-diplomacy/

Chauhan, P. 2019, July 16. *Cooperation against competition: India and China in the energy sector*. South Asian Voices. Retrieved from https://southasianvoices.org/cooperation-against-competition-india-china-energy-sector/

Conant, M. A., & Gold, F. 1978. *The geopolitics of energy*. Boulder, CO: Westview Press.

Conant, M. A., & Gold, F. 1980. *The Geopolitics of Energy* (pp. 45–48). Westview Press.

Druif, M. 2017, November 13. *Energy diplomacy as a form of soft power: The rise and fall of Brazil's ethanol diplomacy in Africa*. Universitat Leiden. Retrieved from https://doi.org/core.ac.uk/download/pdf/141518959.pdf

Druif, M. 2019. *Energy Diplomacy: A Global Perspective on the Role of Diplomacy in Energy Transitions* (p. 16). Clingendael Institute.

Goldthau, A. 2010. Energy diplomacy in trade and investment of oil and gas. In *Global energy governance: The new rules of the game*, edited by A. Goldthau & J. M. Witte (pp. 25–48). Washington, DC: Brookings Press.

Goldthau, A., & Sitter, N. 2018. Conceptualizing the energy nexus in global public policy and international political economy. In *Handbook of the international political economy of energy and natural resources*, edited by A. Goldthau, M. F. Keating, & C. Kuzemko (p. 23). Northampton, MA: Edward Elgar Publishing.

Griffiths, S. 2011. UAE energy diplomacy: Foreign policy with commercial aims? In *Global Energy Governance: The New Rules of the Game*, edited by A. Goldthau & J. M. Witte (pp. 117–137). Brookings Institution Press. (See especially pp. 120–122)

Griffiths, S. 2019. Energy diplomacy in a time of energy transition. *Energy Strategy Reviews*, 26: 55–69.

Hamilton, L. H. 2005. Foreword. In *Energy and security: Toward a new foreign policy strategy*, edited by J. H. Kalicki & D. L. Goldwyn (p. xxi). Washington, DC: Woodrow Wilson Center Press.

Hughes, L. 2020, January 30. Meeting India's energy requirements in 2030. *Future Direction International*. Retrieved from http://www.futuredirections.org.au/publication/meeting-india-s-energy-requirements-in-2030-1/

International Energy Agency. 2019, April. *Chinese companies' energy activities in emerging Asia*. Retrieved from https://iea.blob.core.windows.net/assets/f165f18e-bc05-4cee-8c18-3941799c0a47/Chinese_Companies_Energy_Activities_in_Emerging_Asia.pdf

International Renewable Energy Agency (IRENA). 2019. *A new world: The geopolitics of the energy transformation*.

Joshi, S., & Powell, L. 2018, October. India: Energy geo-politics. Occasional Paper No. 173.

Koyama, K. 2019, March. Energy security and energy politics. *IEEJ Outlook*. Retrieved from https://eneken.ieej.or.jp/data/8373.pdf

Kruse, F. 2014. *Oil politics: The West and its desire for energy security since 1950*. Hamburg: Anchor Academic Publishing.

Madan, T. 2008. India's global search for energy. In *Foreign addiction: Assessing India's energy security strategy*, Asia Program Special Report 142, edited by M. Kugelman (pp. 7–8). Washington, DC: Woodrow Wilson Center.

Madan, T. 2020. *Fateful Triangle: How China Shaped US-India Relations during the Cold War* (pp. 4–7). Brookings Institution Press.

Ministry of External Affairs, Government of India. 2021, May 23. *India-US joint statement on launching the India-US climate and clean energy agenda 2030 partnership*. Retrieved from https://mea.gov.in/bilateraldocuments.htm?dtl/33821/IndiaUS+Joint+Statement+on+Launching+the+IndiaUS+Climate+and+Clean+Energy+Agenda+2030+Partnership

Ministry of New and Renewable Energy, Government of India. 2021, June 23. Retrieved from http://164.100.94.214/international-cooperation

Ministry of Petroleum and Natural Gas, Government of India. 2021, June 20. Retrieved from https://mopng.gov.in/en/international-cooperation/energy-diplomacy

Pant, G. 2015. Introduction: India's emerging energy relations: Issues and challenges. In *India's emerging energy relations: Issues and challenges*, edited by G. Pant (pp. 1–15). New Delhi: Springer.

Pascual, C. 2015, September. *The new geopolitics of energy*. The Center on Global Energy Policy. Retrieved from https://www.eenews.net/assets/2015/09/15/document_cw_01.pdf

Pascual, C. 2015. Power and responsibility: The role of energy in the US Foreign Policy Agenda. In *Energy Security and Global Politics: The Militarization of Resource Management*, edited by D. Moran and M. Russell (pp. 13–29). Routledge

Rajagopalan, R. 2021. Modi sticks to India's nuclear path. *International Politics*. https://doi.org/10.1057/s41311-021-00315-2

Reinhardt, R. O., & Pronichkin, S. V. 2015. Energy diplomacy and international relations: A realist perspective. *International Journal of Energy Economics and Policy*, 5(3): 689–694. (See especially p. 690).

Reinhardt, R. O., & Pronichkin, S. V. 2018. The realist paradigm of energy diplomacy in the Russian scientific tradition and its practical applicability. *MGIMO Review of International Relations*, 58(1): 97–99.

Shen, S. X. H. 2015. Revisiting energy diplomacy: china, energy security and the pragmatic turn in energy diplomacy. *Journal of Contemporary China*, 24(95), 337–355. (See particularly pp. 340–343)

Shen, S. X. H. 2020, March 23. *Qualitative energy diplomacy in Central Asia: A comparative analysis of the policies of the United States, Russia, and China*. The Brookings Institution. Retrieved from https://www.brookings.edu/research/qualitative-energy-diplomacy-in-central-asia-a-comparative-analysis-of-the-policies-of-the-united-states-russia-and-china/

Skeet, I. 1996. Geopolitics of energy. *Energy Exploration and Exploitation* 43(4), 265–272.

10 The Dynamics of Energy and Maritime Security in the Horn of Africa

Red Sea Transits and Geopolitical Implications

Idris Yeba Buta and Tewodros Woldearegay

Background

Since the opening of the Suez Canal in 1869, the Horn of Africa (HoA) has been a focal point for competition and rivalry among great powers. This is due to the region's strategic location at the southwest gate to the Red Sea, where the Bab-el-Mandeb Strait connects to the Gulf of Aden. The Bab-el-Mandeb Strait is one of the world's most critical chokepoints, along with the Suez Canal and the Strait of Hormuz (De Waal, 2018). These three waterways handle significant amounts of global trade, including energy, goods, and weapons. As a result, the HoA plays a vital role in connecting European markets with those in Africa, the Middle East, and Asia. This route accounts for around 10–12% of the global maritime trade, 30% of global container traffic transits, between 1.7 and 5.5 million barrels of oil per day, 40% of trade between Europe and Asia, and over 90% of international trade of most of the countries of the HoA, including Sudan, South Sudan, Ethiopia, Eritrea, Djibouti, and Somalia (Dahir, 2019).

Since the independence of the countries of the HoA in the 1950s and 1960s and the departure of the European colonial powers, external powers with interests and the wherewithal have tried to secure the energy-rich region of the Persian Gulf (the Gulf) as well as the energy and maritime routes from the Strait of Hormuz through Bab-el-Mandeb Strait and Suez Canal by establishing their presence in the HoA (Ylönen, 2022). During the Cold War, both the US and the USSR established military bases in countries of the HoA in exchange for support to their governments. After the end of the Cold War, particularly following the emergence of transnational terrorism as the main threat to energy and maritime security, the US re-established its military presence in the HoA. Furthermore, the region has become a major hub for foreign military bases and naval units since the outbreak of Somali piracy in 2008. In addition to the United States, China, Japan, and France, which have military bases, several countries have established enduring naval presence to protect energy and maritime security in the Red Sea and Indian Ocean. In addition to the UAE, Germany, Italy, Spain, Israel, and Turkey, which have already established their presence in the region, Saudi Arabia and Russia are reportedly

DOI: 10.4324/9781003633204-12

interested in establishing military bases in Eritrea or Djibouti (Carbone, 2020). The emerging dynamics of linking the Red Sea with the Indo-Pacific great power competition and the emergence of the Middle Eastern and Gulf states as geopolitical players have resulted in the further militarization of the HoA.

Different scholars have studied the geopolitical competitions and rivalries between and among external powers to establish their influence or secure the vital energy and maritime routes of the Red Sea, the Gulf of Aden, and the Indian Ocean from different perspectives, mainly from the perspectives of great powers and other external actors. However, the implications of the interaction between energy and maritime security and the geopolitics for the countries of the HoA have not been sufficiently addressed. This chapter explores the implications of the intricate relationship between energy and geopolitics for regional security in the HoA. To achieve this, this chapter is divided into four sections. The first section presents the implications of energy and geopolitics interaction during the Cold War. The second section presents the implications of interventions in the HoA to fight terrorism and Somali piracy. The third section presents the consequences of Gulf powers' interventions in the HoA. The final section briefly touches on the implications of the emerging great power competition, energy security, and geopolitics interaction in the HoA.

Regional Security Implications of the Interaction of Energy Security and Geopolitics: The Horn of Africa during the Cold War

Since their independence following the Second World War, the domestic and regional security policies and relations of the HoA countries have been significantly affected by the Cold War geopolitical rivalries to control the energy chokepoints and maritime security from the Red Sea to the Indian Ocean (Ylönen, 2022). Ethiopia, Sudan, and Somalia tried to leverage their strategic locations to extract significant concessions from one superpower, or sometimes from both, to ensure the incumbent regime's survival and pursue their specific national development and security policies. The attempts by the ruling classes of these countries to use resources provided by Cold War alliances and rivalries institutionalized patterns of proxy wars and interstate wars. These wars led to the collapse, fragmentation, and weakening of the states of the region at the cost of millions of lives and limbs, with impacts still visible (Metaferia, 2009). This section provides a brief overview of the consequences of superpower interventions for energy and maritime security in the HoA during the Cold War, taking the case of Ethiopia and Somalia.

The elites of the HoA started employing tactics of capitalizing on the importance of the Red Sea even before the end of the Second World War. Ethiopia's elite under Emperor Haile Selassie started lobbying for the support of the US as early as 1942 (Carbone, 2020). After three years, the lobbying bore fruit when Haile Selassie leveraged Ethiopia's geopolitical significance and energy security at the Suez Canal meeting with President Roosevelt in 1945. Haile Selassie presented six requests to the president, including access to

the sea through Eritrea, the Ogaden oil deal, and participation in various international initiatives. As a recognition of Ethiopia's strategic importance, the US helped it achieve access to the sea with the Eritrean Federation in 1952. Furthermore, in the same year Washington also included Ethiopia in the Point Four assistance program (Metaferia, 2009).

In the context of the Cold War, the Haile Selassie regime secured the largest American support in Africa by aligning its goals with US strategic interests. Both nations aimed to contain communist influence in the strategically vital Red Sea and Bab-el-Mandeb Strait. Ethiopia acted as a bulwark against communist expansion on this maritime route while also serving its interests by deterring the influence of left-leaning regimes like Ba'athist Syria, Iraq, and Nasser's Egypt. These regimes threatened Ethiopia by supporting the Eritrean secessionist movement and Somali territorial claims against Ethiopia, aiming to turn the Red Sea into an "Arab lake" by landlocking Ethiopia from the Red Sea (Patman, 1990). To secure the vital energy chokepoint of Bab-el-Mandeb Strait from being controlled by pro-Soviet forces, the US signed the Ethiopian - American Mutual Defense Agreement with the Haile Selassie regime in 1953. The United States established several naval and communications facilities, including in Massawa port and Asmara, to control the Red Sea region. Based on this agreement, the US established the Military Assistance Advisory Group (MAAG), training tens of thousands of Ethiopian soldiers and officers. This support transformed Ethiopia into the best-trained army in Africa (Markakis, 2011) and the region's dominant air force, due to US-supplied firepower (Patman, 1990). As a result, Ethiopia received over 60% of total US military aid to Africa (Zewde, 2002). With this enhanced military capability, the Haile Selassie regime effectively thwarted Somali territorial ambitions and suppressed the Eritrean separatist movement and other rebellions in Bale and Ogaden until the regime was deposed by the popular revolution of 1974, which was partly enflamed by the shock of the oil prices of 1973 (Østebø, 2020; Wrong, 2005).

While neighboring Ethiopia grappled with a brewing 1974 revolution and its aftermath, neighboring Somalia, under Siad Barre, embarked on an unprecedented arms race in the HoA, fueled by generous backing from the Soviet Union and its allies. Barre granted the Soviets access to build a military base in Berbera, strategically situated on the Gulf of Aden, giving the Soviet navy and military significant influence over a vital global energy route. In exchange for this strategic concession, Somalia received a massive military upgrade, eclipsing Ethiopia's firepower by a vast margin by 1976 and reshaping the regional balance of power. To illustrate, Somalia boasted three times more tanks, equipped with superior firepower, armor, and range. They also possessed twice the number of armored personnel carriers (APCs) and significantly more combat aircraft, artillery, and ground-to-air missile capabilities. Empowered by this military might, Siad Barre's Somalia invaded Ethiopia in July 1977, swiftly occupying a vast swathe of the Somali-inhabited Ogaden region (Tareke, 2009).

Seeking to halt Somalia's advances and regain the regional balance of power, the Ethiopian military junta, the Derg, leveraged the region's strategic

importance in the context of the Cold War tensions. After ousting Emperor Haile Selassie in the revolution, the Derg saw an opportunity to woo the Soviet Union away from Somalia. This move was particularly strategic due to Ethiopia's greater geopolitical significance. Somalia, already having invaded Ethiopia in July 1977, further solidified Derg's case by expelling Soviet personnel in November and by inviting Washington to replace Moscow (Ayele, 2014). This act and Somalia's territorial claims against Ethiopia convinced the USSR to back the Derg fully. The Soviet Union embraced Ethiopia, seizing the opportunity to replace the United States as Ethiopia's main ally and securing its influence in the Red Sea region. Within just two months, the Soviet Union dramatically outmatched all previous US support to Ethiopia by airlifting over $1 billion worth of weaponry. In addition to weapons, the transfer of 1500 Soviet military advisors and 15,000 soldiers with their commanders, alongside two Yemeni armored battalions totaling 4,000 troops, joined the war on the Ethiopian side (Ayele, 2014). These waves of support resulted in a shift in regional power dynamics, which plunged the HoA into intense competition. This resulted in both interstate war and a series of proxy wars that ultimately led to the collapse of Somalia and the fragmentation of Ethiopia and Sudan. The brutal interstate war between Somalia and Ethiopia, which culminated in the Somali National Army's defeat in October 1978, sent Somalia into a downward spiral from which it has never fully recovered. The immediate impact was a failed coup attempt on April 9, 1978, by disgruntled Somali National Army (SNA) commanders unhappy with President Siad Barre's leadership. This unsuccessful coup marked the end of official Somali nationalism and the resurgence of clan politics as the dominant force in Somali governance (Ingiriis, 2016), dynamic which continues to shape the country to this day.

Ethiopia's military regime exploited clan rivalries among Somalis. They backed the Isaaq-dominated Somali National Movement (SNM). Following a failed coup attempt in 1978, Somali officers formed the Somali Salvation Democratic Front (SSDF) under Colonel Abdullahi Yusuf (Majeerteen clan). Later, Mohammed Farah Aidid (Hawiye clan) established the United Somali Congress (USC), receiving targeted Ethiopian support due to his clan's dominance in Mogadishu (Gebrekal, 2002). These insurgent groups, along with other Ethiopian-backed clan-based organizations, launched attacks into southern Somalia with Ethiopian military expertise and logistical support. Ultimately, Ethiopian-supplied arms and training not only helped topple the Somali dictator Siad Barre's regime but also contributed to the collapse of the Somali state (Ingiriis, 2016).

On the other hand, Ethiopia's alignment with the Soviet Union during the Cold War strained its relations with the United States, which countered, in turn, by strengthening ties with Egypt, Sudan, and Somalia. This left Ethiopia isolated as the only major Soviet proxy in the HoA. In response, the US and its allies backed various Ethiopian rebel groups against the ruling Derg regime. By 1991, Ethiopian insurgent groups had successfully overthrown the Derg, with support from Somalia, Sudan, the United States, and other

regional actors. The insurgents' victory divided Ethiopia into two, with the Ethiopian People's Revolutionary Democratic Front (EPRDF) controlling Addis Ababa and the Eritrean People's Liberation Front (EPLF) controlling Asmara. The United States played a crucial role in brokering a two-year transition process for Eritrea, culminating in a referendum. Eritreans overwhelmingly voted for independence, significantly reshaping the geopolitical landscape in the HoA. Consequently, Ethiopia became the most populous landlocked country in the world (Lyons, 2019).

To sum up, the battle for control over the energy chokepoint of the Bab-el-Mandeb and Red Sea strategic and trade route during the Cold War became one of the key drivers of geopolitical conflicts in Africa as a whole, and in HoA in particular (Woldearegay, 2024). The superpowers, the US and the USSR, courted the countries of the region, eager to establish military bases and deny their rivals access to these vital maritime and energy arteries. This influx of support from external powers dramatically shifted regional dynamics, sparking both interstate and internal wars. By the end of the Cold War, the landscape of the HoA had been irrevocably transformed. Somalia had fractured, Eritrea had gained independence from Ethiopia, and the seeds for South Sudan's eventual secession had been sown.

Impact of Energy Security and Geopolitical Dynamics on Regional Security in the Horn of Africa after the Cold War

After the end of the Cold War, the Red Sea and the Gulf of Aden lost their edge as crucial energy chokepoints and security concerns. This is because the threat of a rival superpower disrupting energy supplies disappeared with the Soviet Union out of the picture. As a result, the strategic importance of the HoA also diminished. This waning of the strategic importance of the region was further solidified by the failed US-led UN missions in Somalia and the infamous "Black Hawk Down" incident, which discouraged further involvement (Gasbarri, 2018). The HoA's relevance to energy geopolitics remained largely dormant until the rise of transnational terrorist networks and Somali piracy, posing new threats to the US and global interests in energy and maritime security of the Indian Ocean, Gulf of Aden, and the Red Sea.

The "Global War on Terror" and Implications of the US Intervention in the Horn of Africa

Post-9/11, energy and maritime security, geopolitics, and their interactions were placed under the US-led counterterrorism campaigns called the "Global War on Terror" (GWOT), targeting transnational networks in the HoA. The countries of the HoA were considered threats because of their lack of capacity to ensure a monopoly over the means of violence. The importance of the HoA and the significance of the countries of the region in GWOT were defined in terms of the history of their engagements with Al Qaeda and networks of

individuals who targeted US interests in the 1990s. The nature of their engagements produced two groups of states (Dazi-Héni & Gouriellec, 2021). One group of states of the HoA group, including Ethiopia, Kenya, and Djibouti, were promoted as the bulwark against terrorism. The second group of states, including Somalia and Sudan, were targeted with counterterrorism measures because of their hosting of individuals with links to Al Qaeda. In the first group of states, Ethiopia, Kenya, and Djibouti used the "War on Terror" to strengthen their security forces and consolidate their positions. Ethiopia, in particular, leveraged US aid to become the dominant regional power. By freezing Ethiopia's insurgent groups' movements and by isolating Eritrea, which hosted them, the US counterterrorism policy further enhanced Ethiopia's stability. As the favorite counterterrorism partner of the US in the region, Kenya also used the US counterterrorism resources to empower its police, defense, security, and counterterrorism forces. Finally, Djibouti reaped benefits by hosting, since 2002, the Combined Joint Task Force-Horn of Africa (CJTF-HOA) as the only US permanent base in Africa (Mamdani, 2009).

The second group of countries, mainly Somalia and Sudan, were targeted with the US counterterrorism policies and programs that had a profound impact on both countries and the region at large. The US, along with the UK and Norway, supported the process of secession of the oil-rich region of South Sudan. The support of the Sudan People's Liberation Movement (SPLM) forced Khartoum to sign the 2005 Comprehensive Peace Agreement (CPA), leading to the formal independence of South Sudan in July 2011. The signing of CPA also inflamed opposition to Khartoum from the Darfur region, resulting in the violent suppression of dissent, prompting international intervention and the establishment of the UN-African Union Mission in Darfur (UNAMID) (Mamdani, 2009). These interventions further fractured Sudan, with effects still reverberating both in South Sudan and Sudan. In the absence of a functioning government in Somalia, the US sought to combat Somali terrorist cells by backing clan leaders and warlords. This strategy backfired, however. Empowered by American support, these warlords carved out personal fiefdoms, fostering corruption and discontent. In response, Somali jihadist groups united under the Islamic Courts Union (ICU) to establish an Islamic state in southern Somalia. The ICU's leadership, including former terrorist leader Sheik Hassan Dahir Aweys, raised concerns in neighboring countries and the US Fears of Taliban-like governance and the ineffectiveness of US-backed warlords prompted Ethiopia to intervene in December 2006 at the invitation of the fledgling Somali Transitional Federal Government (TFG) (Samatar, 2007). Ethiopia swiftly toppled the ICU in less than two weeks during a military intervention in Somalia, deploying a significantly larger and better-equipped force to support the Somali Transitional Federal Government and restore stability in the region. However, the collapse of the ICU prompted the emergence of a more radical Islamist insurgency called Al-Shabaab (Ingiriis, 2018). Furthermore, the defeat of US-supported warlords by the ICU and the collapse of the ICU with Ethiopia's intervention opened a power vacuum that contributed to the outbreak of piracy from the coasts of Somalia.

Somali Piracy, Red Sea Energy and Maritime Security and Militarization of the Horn of Africa

The outbreak of Somali piracy in 2008 posed a significant threat to maritime security in the Indian Ocean, the Gulf of Aden, and the Red Sea. The pirates operating from Somalia conducted hundreds of hijackings and kidnapped thousands of sailors for ransom. This disrupted global trade flows as shipping companies diverted to safer, but more expensive alternative routes to avoid pirate-infested waters. This led to the rising transportation costs for essential goods like oil and gas that were shipped through trade routes accessible to the Somali pirates. Estimates suggest that the annual economic impact of Somali piracy between 2008 and 2012 ranged from $7 billion to $16 billion (Murphy, 2009).

The growing threats of Somali piracy prompted unprecedented interventions by navies of more than 30 countries. Mainly led by non-African forces, these interventions quelled piracy by 2012. Two main types of external actors participated in these anti-piracy efforts, with differing implications for regional stability and power dynamics. One group is the independent counter-piracy missions conducted by China, Russia, India, Iran, Malaysia, South Korea, and other countries. The second category is the US-led anti-piracy coalition which aimed to conflate counterterrorism and anti-piracy. The independent counter-piracy missions were mainly dispatched to fight the piracy menace with naval force units' structure that reflected their mission (Conteh-Morgan, 2019). Contrary to the independent counter-piracy missions, the US-led anti-piracy campaigns involve multiple purposes and multiple assets and sometimes include other partners or institutions. First, the counter-piracy mission was an extension of the counterterrorism objectives. In addition to its resources, the US capitalized on NATO warships in October 2008 to patrol the waterways of the HoA. Instead of relying on naval forces, the US deployed surface and air assets to support the naval units. Furthermore, the US Navy established Combined Task Force (CTF) 151, a multinational naval partnership mandated to secure and protect the waterways from the Strait of Hormuz to the Red Sea. Moreover, the US also employed regional clan leaders and warlords as anti-piracy forces in the coastal areas of their region. This strategy of relying on regional leaders for counterpiracy led to an unintended consequence of undermining the unity of the Somali state (Ploch et al., 2011).

The unintended outcome of international support for anti-piracy initiatives in Somalia is the emboldening of regional governments and increased political fragmentation. The external actors provided capacity-building technical and arms support for strong and relatively stable regions like Puntland and Somaliland. The foreign support further emboldened the regional states to establish their own defense, security, and counter-piracy forces independent of the federal government. The feeble federal government could not exert its authority and maintain a cohesive national governance structure. On the other hand, with their growing capacity and the inflow of international resources, the regional states asserted their autonomy. This has contributed to political fragmentation within Somalia, making it more challenging for the federal

government. In summary, while external actors' anti-piracy endeavors have successfully reduced piracy along Somalia's coast, they have inadvertently strengthened regional states and exacerbated political fragmentation within the country (Van Ginkel & Van Der Putten, 2010).

The external interventions in the HoA to fight Somali piracy led to the militarization of the HoA as external powers competed to open naval and military bases across the HoA. While the foreign forces established their naval and military bases with the invitation of Djibouti, Eritrea, and Somalia (Somaliland), the concentration of foreign military facilities has already de-Africanized the waters of the HoA. None of the coastal states of the HoA, Sudan, Eritrea, Djibouti, and Somalia, have the naval capacity to provide maritime security as a public good beyond their coastal zone. This has two major consequences. First, militarization of the region also undermines the AU's African Integrated Maritime strategy that calls for regional integration to ensure maritime security. Second, the placement of African ports under the influence of foreign actors, including competing great powers like the US and China, has created a threat to landlocked Ethiopia's freedom to access and use Djibouti port using a railway between competing great powers a few kilometers apart. Furthermore, external powers' militarization of the HoA was further complicated by the intervention of the Gulf states to protect their energy and maritime security of the Indian Ocean, Gulf of Aden, and the Red Sea. These are the Gulf powers (Conteh-Morgan, 2019).

Persian Gulf Powers' Rivalries and Militarization of the Horn of Africa

While the Gulf states, mainly Saudi Arabia, Iran, Qatar, and UAE, have been part of the energy-geopolitics nexus of the HoA due to its proximity to energy transit from the Strait of Hormuz through the Red Sea to Europe, their autonomous interventions into the region with significant repercussions were recent phenomena. After 2014, a convergence of factors prompted Gulf States to pursue independent strategic engagements in the HoA, marking a shift from the historical norm of close alignment with the interests of external great powers, principally the US. The 2014 intervention in Yemen catalyzed Gulf states' assertiveness in the HoA with other driving factors (Vertin, 2019).

First, in 2011, the US announced its strategic pivot to Asia, leaving a perceived security vacuum in the strategy of vital energy and trade routes from the Strait of Hormuz through the Bab-el-Mandeb Strait to the Suez Canal. Feeling less assured of US commitment, Gulf States stepped up their own involvement to fill the void (Melvin, 2019). Second, Iran's growing presence in the Red Sea, particularly its support for Houthi rebels in Yemen, is seen as a direct threat by Gulf States. They aim to counter Iranian influence and secure their regional strategic interests (Mabon & Mason, 2022). Third, Turkey's expanding economic and diplomatic footprint in Somalia and Sudan has also spurred Gulf engagement. Some Gulf States view this expansion with

suspicion and seek to maintain their own influence in the region (Başkan, 2016). Fourth, China's ambitious infrastructure project, the Belt and Road Initiative (BRI), has prompted the United Arab Emirates (UAE) to invest heavily in ports and logistics infrastructure in the HoA, particularly in Djibouti and Eritrea. This is partly driven by the fear of being excluded from key trade routes and economic opportunities (Vertin, 2019).

Even though several material and ideological interests led to the intervention of the Gulf States in the HoA, the uniting factor was the shared threat of Iranian influence. To remove possible scenario of the threat of where Iran was in a position to block both the Strait of Hormuz and the Strait of Bab-el-Mandeb using their Houthi proxy in Yemen, the Saudi-led coalition strongly pressured or coerced the Horn of Africa countries to cut diplomatic relations with Iran. They used their financial leverage (Riyal Politik) to induce the countries of the HoA to cut ties with Iran (Mabon & Mason, 2022). They were able to turn all coastal states against Iran. Furthermore, Somalia, Djibouti, and Eritrea allowed their ports and airspaces to be used by the Saudi-led coalition war against Houthis in Yemen. Moreover, Sudan provided Rapid Support Forces (RSF), a paramilitary force led by Mohamed Hamdan Dagalo (Hemetti) in the war against the Houthis. Their policy was successful in blocking Iran from accessing the Red Sea. However, the Saudi-led coalition failed to defeat Houthi rebels. As they bogged down in an unending war in Yemen, fault lines started to emerge within the coalition itself. These tensions eventually boiled over into intra-Gulf rivalries, particularly between the Saudi Arabia and Qatar (Başkan, 2016). In contrast to Tehran, which the coalition had largely unified against earlier, applying pressure was not enough to turn the HoA nations against Doha. This led to the UAE taking drastic measures against Somalia, a country with closer ties to Turkey and Qatar. Somalia bore the brunt of the UAE's frustration. Refusing to sever ties with Doha, as Abu Dhabi demanded, Somalia faced swift repercussions. The UAE abruptly cut relations with the federal government and halted all development projects, including vital hospital and military training facilities. Moreover, the UAE actively began supporting regional Somali states against the federal government, further fueling the fragmentation of Somali politics (Mabon & Mason, 2022).

Furthermore, the UAE played a significant role in fueling the war in Ethiopia and in derailing the democratic transition in Sudan. The UAE provided drones, weapons, and finance in support of Ethiopia's federal government war against the Tigray People's Liberation Front (TPLF) insurgents in Tigray. Abu Dhabi's support fueled and dragged the Tigray war, contributing to the killing of hundreds of thousands and the destruction of infrastructure and property in Ethiopia (Gebru, Zeru, & Tekalign, 2023). Similarly, Abu Dhabi and Riyadh bankrolled the army hijacking of the democratic transition in Sudan and subsequent in-fighting between the armed forces: the SNA led by Burhan and the UAE-backed RSF led by Hemetti (Gebru, Zeru, & Tekalign, 2023). Given the power vacuum created by the absence of a great power willing to provide strategic leadership in the region, the Gulf states like the UAE, with deep pockets,

will likely continue to exert significant influence with deleterious consequences in the HoA. The exception to the negative consequences of the Gulf states' intervention in the countries of the HoA was their role in the rapprochement between Ethiopia and Eritrea, which was principally driven by Eritrea, since it saw an opportunity in the Gulf States' involvement in the HoA. To get the UN sanctions lifted, improve its regional standing, and get financial and arms support, Eritrea cut ties with Iran to show its commitment to aligning with the Gulf States' interests. Asmara also provided military support for the war in Yemen by allowing access to its Assab port and airspaces. In return, the Gulf States provided Eritrea with much-needed financial assistance and played a crucial role in brokering the historic peace agreement with Ethiopia (Mabon & Mason, 2022). They sponsored the peace deal, which was signed in Abu Dhabi and Jeddah. It was a new development for African countries to sign peace agreements outside the African regional organizations, IGAD, or the African Union. Even the positive contribution of the Gulf states in the HoA is at the cost of undermining the norm of "African Solution to African Problems".

Emerging Great Power Competition, Energy Security, and the Horn of Africa

Simultaneously with growing interventions of the Gulf states in the HoA in relation to energy and energy routes security, a great power competition is emerging with far more profound and broader implications for the security of the HoA and the Red Sea. The great power competition, principally between the US and China, is already pulling the Red Sea and HoA into the Indo-Pacific security dynamics, the focal point of the emerging great power competition (Gurjar, 2022). This vast region, stretching from the western coast of the United States to the Red Sea's western shores in the HoA, pulsates with vital sea lanes, serving as the arteries of global trade connecting East and West (Vertin, 2020). By encompassing energy chokepoints like the Suez Canal, the Bab-el-Mandab Strait, the Strait of Hormuz, and the Strait of Malacca, the Indo-Pacific is emerging as the central stage on which the US, China, Europe, Japan, India, and other powers navigate, compete, and potentially collaborate to shape the future of the global order.

As the cradle of the majority of the world's population, the largest share of global wealth, and the most extensive proven fossil fuel reserves, the Indo-Pacific attracts the strategic maneuvering of leading powers vying to maximize their interests, influence, and market shares. Recognizing this shift, the United States has redefined the Indo-Pacific as a unified strategic theater to maintain its dominant position. Renaming its Pacific Command to Indo-Pacific Command in 2018 underscores this commitment. Partnering with allies like the EU, Japan, and South Korea, the US is actively balancing China's growing influence, including on the HoA's maritime waterways, the Indian Ocean, the Gulf of Aden, and the Red Sea. Despite the decline in Somali piracy since 2012, the naval and military facilities of the US and its allies in the HoA have undergone

improvements and upgrades. This trend intensified after China's 2017 inauguration of its first overseas military base in Djibouti. For instance, the US and Japan significantly invested in enhancing their bases in relation to this development (Melvin, 2019).

China, the primary target of the Indo-Pacific region's redefinition, is also actively fostering integration through its BRI. By pouring billions into horn countries, China financed port expansions, railways, and the development of energy sources and power plants. By building these development infrastructures, China will be able to establish long-term influence and secure access to resources in these countries (Wan et al., 2020). While these development infrastructures were mainly aimed at the economic integration of the countries of the HoA with the Chinese economy, there is an overall trend of shifting towards strategic competition and power projection, as can be attested by the establishment of the first overseas military base in Djibouti in 2015. This base strategically positions China less than twenty kilometers north of the US and Japanese military facilities, making it a significant move in China's broader strategic ambitions. This Chinese military facility provides several strategic purposes, including protecting its citizens and businesses in the region, safeguarding the vital sea lanes of the Red Sea to protect its commercial and strategic interests, and projecting military power beyond its immediate borders (Melvin, 2019).

The US is becoming increasingly concerned about China's expanding military presence in the HoA because it sees this as a challenge to its hegemony in the Red Sea and Bab-el-Mandeb Strait. Additionally, the US military's freedom of movement across critical theaters, including territories under the Indo-Pacific Command, Central Command, and Africa Command, might be disrupted by China's rising influence. Furthermore, China is already involved in the great power competition over the HoA as a source of energy through its investments in the development of energy resources in Sudan, South Sudan, and Ethiopia as well as its interests in the development of recently discovered oil and gas reserves in Somalia and Kenya. This competition for dominance in the HoA is expected to intensify as China, the US, and other powers seek to secure their strategic interests, including the HoA's potential as a source of minerals required for energy transition (Woldearegay, 2024).

In this emerging great power competition and the moves that are pulling the HoA into the Indo-Pacific security dynamics, the countries of the HoA have not been mere spectators or pawns in the emerging geopolitical competition. Rather than being passive observers in this geopolitical contest, the countries of the HoA have actively engaged and initiated their own strategies to benefit from the involvement of external powers while safeguarding their sovereignty and interests. For instance, Djibouti, a city-state of fewer than one million people, strategized on its strategic location to invite China to establish the military base in addition to already established French, American, and Japanese military bases. By hosting military bases of all the great powers, except Russia, Djibouti is earning substantial rent, reaching US$100 million and counting, as well as additional international resources flowing in the range of US$200–300

million dollars annually (Vertin, 2020). This gave Djibouti a considerable latitude of policy independence from dependence on Ethiopia's port use rents. Furthermore, Djibouti's policy of hosting multiple foreign military bases ironically gave it security from more powerful neighbors, Ethiopia and Eritrea.

Additionally, the HoA presents a unique landscape where countries like Ethiopia, Djibouti, and Kenya engage with external powers based on a clear-eyed assessment of their own interests. This pragmatic approach prioritizes maximizing national gains over unwavering loyalty to any one superpower. For instance, Ethiopia has been partnering with the United States in counterterrorism efforts and regional peacemaking initiatives like Sudan, Somalia, and South Sudan, conflicts that align with its security priorities. Simultaneously, Ethiopia has become one of the largest beneficiaries of Chinese development partnerships, leveraging billions of dollars in investments for infrastructure projects like railways, roads, telecommunications networks, and power grids (Chakrabarty, 2016). This diversified engagement reflects Ethiopia's strategic balancing act, optimizing partnerships with the West and the East to propel its development agenda. Similarly, Djibouti hosts US and Chinese military bases alongside significant investments from both powers in its ports and infrastructure. Kenya has also received significant Chinese investment in its transportation networks and energy sector while maintaining close security ties with the West. These examples highlight the nuanced reality of international relations in the HoA, where the region's countries follow pragmatism to navigate a complex global landscape to secure their own national interests.

However, the increasing intensity of the great power competition with a corresponding carrot and stick may undermine the current strategies of nonalignment by countries of the region. The infusion of significant external resources and pressures from powerful actors will likely affect the relationship between countries of the region by changing the regional balance of power. Simultaneously, proxy conflicts resourced by great power competition, in both internecine and cross-border forms, may trigger fault lines, including religious and ethnic tensions that may lead to civil and interstate conflicts. This can occur when influential foreign powers compete with each other, which can worsen existing conflicts or even trigger new ones. This will likely destabilize the region, as was the case during the Cold War, US counterterrorism interventions, militarization after the outbreak of Somali piracy, as well as intervention by the Gulf states in Somalia and Sudan (Carbone, 2020).

Conclusion

This chapter explored the complex interplay between energy, geopolitics, and interventions in the HoA, a strategically important region in the global south. Both global powers and regional actors have long sought to secure or control the vital energy and maritime routes from the Suez Canal through the Bab-el-Mandeb Strait to the Strait of Hormuz. This has often led to interventions, including by invitation, in the countries of the HoA, with

significant consequences for the region's stability and balance of power. During the Cold War, interventions by superpowers enabled interstate and proxy wars that led to the collapse of Somalia, the secession of Eritrea, and the fracturing of Sudan. More recently, US interventions in the name of fighting terrorism have contributed to the secession of South Sudan and the further fragmentation of Somalia and Sudan while also strengthening neighboring countries like Djibouti, Ethiopia, and Kenya. The outbreak of Somali piracy in 2008 led to the militarization of the HoA, which further destabilized Somalia. Since 2014, interventions by Gulf States have solidified the fragmentation of Somalia and Sudan, but they have also helped to improve relations between Eritrea and Ethiopia and end Eritrea's isolation. As countries in the HoA emerge as potential sources of fossil fuels and minerals important for the energy transition, foreign powers will likely continue to intervene in the region in the context of global power transition and emerging great power competition. Given the history of interventions and their often-dire consequences, it is likely that these interventions will have a significant impact on the region's stability and future.

References

Ayele, F. 2014. *The Ethiopian army: From victory to collapse, 1977–1991*. Northwestern University Press, Evanston, IL.

Başkan, B. 2016. *Turkey and Qatar in the tangled geopolitics of the Middle East*. Springer, The New York.

Carbone, G. 2020. A new Horn: Still thorny. In *Africa's thorny Horn: Searching for a new balance in the age of pandemic*: 13–30. Stockholm International Peace Research Institute, Stockholm.

Chakrabarty, M. 2016. Ethiopia–China economic relations: A classic win–win situation? *World Review of Political Economy*, *7*(2): 226–248.

Conteh-Morgan, E. 2019. Militarization and securitization of Africa: The role of Sino-American geostrategic presence. *Insight Turkey*, *21*(1): 77–94.

Dahir, A. H. 2019. *Foreign engagements in the Horn of Africa: Diversifying risks and maximising gains*. TRT World Research Centre, Turkey.

Dazi-Héni, F., and Gouriellec, S. L. 2021. The Red Sea: New spaces of interdependent security issues between countries of the Gulf and of the Horn of Africa. *IRSEM: The Institute for Strategic Research at the Military School*. https://www.irsem.fr/media/5-publications/notes-de-recherche-research-papers/rp-irsem-75.pdf

De Waal, A. 2018. Beyond the Red Sea: A new driving force in the politics of the Horn. *African Arguments*, *11*. https://africanarguments.org/2018/07/beyond-red-sea-new-driving-force-politics-horn-africa/

Gasbarri, F. 2018. From the sands of the Ogaden to Black Hawk Down: The end of the cold war in the Horn of Africa. *Cold War History*, *18*(1): 73–89.

Gebrekal, M. 2002. *The Horn of Africa: The changing nature of security in the aftermath of the Cold War* (Doctoral dissertation, University of London).

Gebru, M. K., Zeru, G., & Tekalign, Y. 2023. The impact of the Middle East and Gulf States' involvement on the Horn of Africa's peace and security: Applying regional security complex theory. *Digest of Middle East Studies*, *32*(3): 223–245.

Gurjar, S. 2022. *The superpowers' playground: Djibouti and geopolitics of the Indo-Pacific in the 21st century*. Routledge, India.

Ingiriis, M. H. 2016. *The suicidal state in Somalia: The rise and fall of the Siad Barre regime, 1969–1991*. University Press of America. New York.
Ingiriis, M. H. 2018. From Al-Itihaad to Al-Shabaab: How the Ethiopian intervention and the 'War on Terror' exacerbated the conflict in Somalia. *Third World Quarterly*, *39*(11): 2033–2052.
Lyons, T. 2019. *The puzzle of Ethiopian politics*. Lynne Rienner Publishers, Colorado.
Mabon, S., & Mason, R. 2022. *Gulf States and the Horn of Africa: Interests, influences and instability*. Manchester University Press, Manchester.
Mamdani, M. (2009). Saviors and survivors: Darfur, politics, and the war on terror. *African Sociological Review*, *14*(2): 110–113.
Markakis, J. 2011. *Ethiopia: The last two frontiers*. Boydell & Brewer Ltd., United Kingdom.
Melvin, N. 2019. *The new external security politics of the Horn of Africa region*. Stockholm, Sweden.
Metaferia, G. 2009. *Ethiopia and the United States: History, diplomacy, and analysis*. Algora Publishing, New York.
Murphy, M. N. 2009. *Small boats, weak states, dirty money: Piracy and maritime terrorism in the modern world*. Columbia University Press, New York City.
Østebø, T. 2020. *Islam, ethnicity, and conflict in Ethiopia: The Bale insurgency, 1963–1970*. Cambridge University Press, Cambridge.
Patman, R. G. 1990. *The Soviet Union in the Horn of Africa: The diplomacy of intervention and disengagement*. Cambridge University Press, Cambridge.
Ploch, L., Blanchard, C. M., O'Rourke, R., Mason, R. C., & King, R. O. 2011. *Piracy off the horn of Africa*. Library of Congress, Congressional Research Service, Washington, D.C.
Samatar, A. I. 2007. Ethiopian invasion of Somalia, US warlordism & AU shame. *Review of African Political Economy*, *34*(111): 155–165.
Tareke, G. 2009. *The Ethiopian revolution: war in the Horn of Africa*. Yale University Press.
Van Ginkel, B., & Van Der Putten, F. P. 2010. 8. Conclusion: Challenges and opportunities. *The International Response to Somali Piracy*, *30*, 179–187.
Vertin, Z. 2019. Red Sea rivalries: The Gulf states are playing a dangerous game in the Horn of Africa. *Foreign Affairs*, *15*. https://www.foreignaffairs.com/articles/east-africa/2019-01-15/red-sea-rivalries
Vertin, Z. 2020. Great power rivalry in the Red Sea: China's experiment in Djibouti and implications for the United States. *Global China*, *6*, 1–31.
Wan, Y., Zhang, L., Xue, C. Q., & Xiao, Y. 2020. Djibouti: From a colonial fabrication to the deviation of the "Shekou model". *Cities*, *97*: 102488.
Woldearegay, T. 2024. An offensive realism approach to navigate the changing dynamics of summit-level dialogue between the AU and great powers. *Cogent Social Sciences*, *10*(1): 1–15.
Wrong, M. 2005. *I didn't do it for you: How the world betrayed a small African nation*. Fourth Estate, London.
Ylönen, A. 2022. A scramble of external powers and local agency in the Horn of Africa. *Notes Internacionals CIDOB*, *280*: 1–7.
Zewde, B. 2002. *A history of modern Ethiopia, 1855–1991*. Ohio University Press, Ohio.

11 Russia–Ukraine War and the Geopolitics of Energy

Zeeshan Munir

Introduction

The February 2022 Russian invasion of Ukraine has refocused attention on the economic and geopolitical importance of energy. Along with the armed conflict, a parallel war ensued in the energy market, where Russia challenged the rest of Europe. The invasion was followed by punitive Western sanctions, with the aim of crippling Russian power and finance. The European countries tried to reduce their dependence on Russian energy. Broadly, the Western approach was based on the premise that the Russian dominance of the European energy market fuels its hostile posture in the region and helps bankroll its war in Ukraine. Coincidentally, Russia has also earned a reputation as an unreliable supplier, owing to its previous record of cutting gas supplies to Ukraine and Europe in 2006 and 2009 over gas price disputes.

Meanwhile, with its abundant energy resources, location, and distribution network, Russia is comfortably placed as the primary supplier for Europe. These, in turn, offer it a political tool besides economic incentives in the European market. Countering the Western sanctions, Russia imposed its set of restrictions, resulting in supply disruption and exacerbated concerns for Europe's energy security. The European rush to find an alternative supplier further led to an upsurge in international fuel prices. These soaring fuel prices viciously contributed to the global recession and inflation. In these contexts, the present study examines the three intersecting themes of (a) the geopolitics of energy, (b) Russia–Europe energy dependence and confrontation, and (c) the energy politics shaping the Russia–Ukraine war. The study relies on primary and secondary data and concludes that denting Russia's position as the key supplier for European energy requirements remains a long-drawn-out process. The sanctions imposed by the West will put limited pressure on Russia to alter its confrontational behaviour.

Geopolitics of Energy

The 'geopolitics of energy' examines the many ways in which economics, energy, international politics, and security are intertwined. It is based on the assumption that energy, through its availability and supply, impacts the global

DOI: 10.4324/9781003633204-13

system and alliances. Access to energy resources is critical to the rise and fall of a state's power and determines the outcome of wars. Therefore, the critical geopolitical issue is to ensure energy production, distribution, supply, and consumption. Within this context the term "Geopolitics of Energy" can be defined as "the effect that location of resources has on the politics" (Skeet, 1996, p. 265). As quoted in *The Economist*, the 'geopolitics of energy' is described as "the impact of energy flows on the power and influence of nations" (Economist, 2018). These definitions essentially assign the influence of geopolitics to a description of a state's energy strategy. One significant portion of this focuses on energy security owing to the role of energy as a driver of economic growth and stability. According to the International Energy Agency (IEA), 'energy security' is defined as "uninterrupted availability of energy sources at an affordable price" (IEA, 2023). Energy security encompasses various dimensions, with long-term energy security primarily focusing on the appropriate allocation of investments to meet energy demands in accordance with economic advancements and environmental imperatives. Conversely, short-term energy security pertains to the capacity of the energy system to rapidly respond to abrupt shifts in the equilibrium between supply and demand (IEA, 2023). The four main components of energy security, commonly known as the 4A's of energy security, consist of *Availability, Accessibility, Acceptability, and Affordability*.

Energy has a significant role in shaping the outcomes of a state's foreign policy and can also serve as a strategic instrument in pursuing foreign policy objectives. The inclusion of 'energy supply security' in the national security agenda of energy-importing governments and the emphasis on ensuring stable markets in the policy agenda of exporting states are both critical objectives. The consistent availability of oil resources, even in times of armed conflict, is a crucial element in formulating military strategies and national security doctrines—conversely, the absence of such access results in a reduction of military capabilities. During periods characterized by constrained conditions in the international energy market, energy assumes a more critical role as a factor and instrument in the foreign policies of states, thereby acquiring greater priority on their policy agenda. During contemporary times, energy requirements influence the foreign affairs of both importing and exporting nations (Shaffer, 2009, p. 28).

In that sense, states with abundant energy reserves have considerable influence in international affairs, but those reliant on imports are susceptible to price fluctuations and supply interruptions. Irrespective of this, it creates a consumer–producer interdependence where both exporter and importer countries depend on each other: the former needs a good market for energy exports, while the latter requires a steady supply. Historically, states have been more concerned about the danger to supply rather than the threat to pricing (Skeet, 1996, p. 265). Therefore, energy resources multiply the state's power while a lack thereof undermines its relative position in the international system, influencing global security.

The geopolitical significance of energy is also reflected in the state's strategic behaviour. For example, Russia, with one of the world's largest energy reserves, has used them to advance its power and influence in its neighbourhood and Europe. Similarly, the USA is strategically enhancing its domestic production by gradually harnessing renewable sources of energy and shale reserves to cap its dependence on foreign energy sources. In comparison, EU countries' heavy reliance on Russian energy exposes their vulnerability. Energy-producing/-controlling states sometimes use energy resources as a political tactic to exert their influence. For instance, Iran's threats to obstruct oil transport via the Strait of Hormuz and Russia's supply decrease due to the continuing conflict in Ukraine. The role of energy resources in international strife is another crucial facet of energy geopolitics. The Gulf War, the Iraq War, the Libyan War, the Syrian War, and maritime tensions in the South China Sea were greatly influenced by rivalries to control the region's petroleum supplies. Evidently, geopolitics and energy security are intimately interwoven.

The discovery of coal in the 1800s ushered in an age of industrialization for nations with significant deposits, while the transition to oil elevated the Middle East's geopolitical significance. Further, the rise of global warming and climate change has dramatically affected the energy landscape. There is now a demand for the exploration of alternative energy sources and investments in green energy. It will bring new challenges for the energy market and energy-producing states. These changes confirm that the evolution of the geopolitics of energy has coincided with discoveries in energy sources. However, despite the desire to move away from fossil fuels, oil, and gas will remain dominant in the global energy mix because of their demand, which is a driving factor in global security, prosperity, and international politics. Consequently, energy geopolitics represents a complex field that has a bearing on the state's security, power dynamics, and economic strength. Understanding the geopolitics of energy is crucial for guaranteeing energy security and fostering sustainable economic development. It becomes necessary because the global energy landscape is transforming and witnessing rapid energy consumption. Currently, the OPEC (2025) data, as retrieved from Statista, concludes that the global demand for crude oil in 2024 stood at 103.75 million barrels/day, with a projected increase to 105 million barrels/day in 2025. In 2020, it witnessed a slump of 91.91 million barrels/day due to Covid-19, but it has risen in each subsequent year, to 97.08 (2021), 99.57 (2022), and 102.21 (2023) (OPEC, 2025).

Russia–Europe Energy Dependence and Confrontation

The ongoing war in Ukraine also reflects a geopolitical contestation of energy and significantly impacts energy relations between Russia and the EU. Western European countries scrambling to fill the gap due to the Russian supply shortfall have brought back the availability of alternative delivery partners for Europe's energy requirements. In the race, the United States has emerged as the major frontrunner, spearheading efforts to redirect energy supplies to Europe

(McBride, 2022). Simultaneously, the war has severely compromised Ukraine's position as a transit country for European energy imports. Additionally, the destruction of the Nord Stream-2 pipelines reduced the level of Russian exports to Europe. These developments warrant a study to understand the dynamics of Russia–Europe's energy dependence and why it is currently on a path of confrontation.

Where Does Russia Stand in the Energy Sector?

Russia is a major producer of energy; it is often referred to as an "energy superpower" (McBride, 2022; Tsafos, 2018, p. 2). It possesses abundant natural resources and is undisputedly a significant player in the global energy market, being among the world's top three crude producers. It has the world's largest known natural gas reserves, and is the world's second-largest gas producer, as well as its largest exporter. It also has the second-largest coal and the seventh-largest oil reserves. At present, Russia makes up 14% of the world's total crude oil supply. Most of its oil and gas production facilities are in the western and eastern Siberian regions, providing an easy gateway for exports. In terms of major importers, Russia is the largest exporter of oil to China (1.6 million bpd), while Europe receives the major chunk of Russian oil exports (2.4 million bpd) (International Energy Agency, 2022; McBride, 2022).

During the period January–October (2022), Russia exported 51% of its crude oil to Asia, while the EU received 42%. During the same period, the EU received the highest proportion (52%) of Russian seaborne refined petroleum products (EIA, 2023a, p. 11). In 2021, Russia supplied about 40% of the European Union's natural gas consumption, accounting for 45% of imports. With declining domestic natural gas output in Europe, this proportion has grown in recent years. Germany, Turkey, and Italy are the top three markets for Russian natural gas exports (International Energy Agency, 2022). The country has an extensive pipeline network for energy exports, efficiently shipping large volumes directly to Europe and Asia. Its Druzhba pipeline system is the world's most extended pipeline network, estimated to be 5500 km long, and transporting 750,000 bpd of crude oil to refineries in east and central Europe. Russia also operates the ESPO pipeline (4740 km long, and transporting 1.6 million bpd), which helps as a pivot in Asia meant to diversify Russian exports and exploit the Asian market. Russia also transports significant crude oil through ships, tankers, and rail networks.

Russia's Power of Siberia pipeline (3,000 km long and with a capacity of 38 billion cubic meters) was officially opened in 2019 to export directly to China. The goal was to broaden Russian gas exports while decreasing their dependency on European clients. Russia is also increasing its LNG output. In 2021, with around 40 bcm of LNG export, it was ranked fourth in the world for LNG exporter countries (International Energy Agency, 2022). Russia has been expanding oil and gas production in the Arctic to offset decreases at older producing locations. According to current figures, at present it produces 80% of its

natural gas and 20% of its oil in the Arctic. This also gives the country more access to Arctic trade channels, enabling seaborne fossil fuel delivery to Asia. Rosneft is the largest state-owned oil-producing company in Russia, while another state-owned company, Gazprom, covers the gas sector, accounting for around 68% of the production share (International Energy Agency, 2022). The control of these firms by the Russian state lends credence to claims that they are a government proxy. Indeed, Gazprom is often labeled as the strategic arm of the Russian energy apparatus, controlling a quarter of European production and around 4% of UK production.

Russia–Europe Energy Dependence

Russia's substantial resources support its global position in the energy market. The European Union is Russia's largest energy market. It relies on Russian fossil fuel imports for energy needs, while Russia depends on them for market and revenue. This interdependence was a key reason why the Russian energy industry was excluded from the sanctions imposed after the 2014 Crimean annexation (Rossbach, 2018, p. 60). Addressing these concerns, the European Union published the *European Energy Security Strategy* in May 2014. This paper determined that the primary obstacle to European energy security arises from the increasing reliance on a limited number of suppliers, with Russia being the predominant source. Nevertheless, the main challenge faced by the European Union in its efforts to enhance energy security is the need to reconcile varying energy interests and requirements among its member states in order to establish a cohesive energy sector (Rettig & Eran, 2018, p. 103).

Interestingly, not all EU members depend on Russian energy to the same degree. It is East and Central Europe that consumes the bulk of Russian energy. Eastern European countries, such as Bulgaria, the Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Slovakia, and Slovenia, exhibit a significant dependence on imports from Russia, principally in the form of natural gas. The reliance on external sources has made them considerably vulnerable to disruptions in supply, which might be the result of political, commercial, or technological factors. The 2009 political and commercial conflict between Russia and Ukraine is a notable example of this, resulting in a 13-day period of supply disruptions (Parfitt, 2009). Consequently, Ukraine and several Southeast European nations experienced deprivation of natural gas for heating purposes.

In comparison, Western European countries are relatively independent of Russian gas. They are presently reluctant to spend EU money on infrastructure to help East Europe diversify away from Russia because they do not see it as their problem. This creates a rift between West and East Europe that has prevented the EU from taking real action to reduce its dependence on Russia. The variance observed between Eastern and Western countries within the EU presents a significant challenge in formulating a cohesive energy policy for the entire continent. This disparity serves as a source of conflict, further complicating the process of developing a unified approach to energy matters.

At the same time, the 2014 annexation also became a rallying ground for Europe to reduce dependence on gas imports by increasing energy efficiency and diversifying local production. Nevertheless, all those discussions on diversifying and modernizing Europe's energy infrastructure have yet to see much progress. Energy accounted for 62% of EU imports from Russia in 2021 (Early & Saush, 2022). Russia contributes around one-third of European natural gas for winter heating, power generation, and industries. It also supplies 25% of the EU's crude oil imports. Despite best efforts, Europe relies heavily on Russian energy, particularly Germany, which gets more than 30% of its crude oil and more than half of its natural gas from Russia (McBride, 2022). Russia is taking advantage of cracks in the European Union caused by Germany's focus on protecting its gas supply rather than that of Eastern Europe. Many countries in Eastern Europe have extended or expanded their gas contracts with Russia in order to take advantage of cheaper Russian gas. Eastern European nations are sceptical of collective efforts to build a cohesive approach in the energy sector, as is seen from their contempt for EU norms to lessen reliance on Russia (Rettig & Eran, 2018, p. 105).

It is perhaps worth considering here the separation of oil and gas because they behave very differently. Oil is liquid and relatively easy to ship anywhere, making it a global commodity. If the EU does not want to buy Russian oil, it can get oil from the Middle East instead, and Russia, in turn, can sell its oil to China. Oil is also used for different things than gas, mainly transportation, chemicals, and industry (but not for heating or electricity). In contrast, natural gas is much more complicated because it requires permanent pipelines to transit (because it is not liquid), so it is primarily a regional fuel. You can technically liquify it to LNG, but this is a costly process. Thus, the EU cannot simply decide to stop buying gas from Russia as they need to build expensive pipelines. Also, gas is used in Europe mainly for heating and electricity, so the demand for gas is seasonal, It peaks during winter, but Europe needs much less gas during the summer (compared to oil, where the demand is more constant). Thus, in terms of Russia–EU sanctions, natural gas is a much more complicated issue than oil. Russia is much more willing to use gas as a political weapon against Europe, because it knows that the EU has sufficient alternatives for oil.

It is important to note that states rarely have more than one natural gas supply infrastructure due to the significant expenses of developing these infrastructures. Consequently, states are theoretically dependent on suppliers and they may be exploited by these providers for political and security purposes. Customers cannot easily switch between different suppliers. Changing the fuel source, such as switching from natural gas to coal or oil to generate electricity, may be their only option. As a result, there is interdependence between nations that utilize energy and those that supply it in long-term natural gas contracts. Energy is provided by suppliers to consumers, who give a market for those services to those who offer them (Shaffer, 2009, pp. 38–39).

According to some estimates, oil and natural gas contribute around 45% of revenues to the Russian federal budget, and fossil fuels have a 14% share in the country's economic output (International Energy Agency, 2022); McBride,

2022). Russia generates more money from oil than gas since it sells the majority of its oil but just a third of its gas. Russian control over gas prices makes it a more potent foreign policy weapon for the Kremlin. Over the years, Russia's economy and exports have grown more reliant on the sale of fossil fuels, which make up more than two-thirds of all Russian exports (Dreyer et al., 2014, p. 39). Russian energy analyst Jonathan Stern holds that the European gas market is the most crucial "geopolitical aspect" of Russia's energy ties with Europe. The Russian energy relationship with Europe contributes significantly to the Russian economy and also bolsters the country's global status (Rossbach, 2018, p. 60).

Hence, notwithstanding the European Union's diligent endeavours, it is probable that in the foreseeable future Russia will persist as the principal natural gas supplier to Europe. A vast network of pipelines spanning thousands of kilometers facilitates the transportation of affordable and easily accessible gas from Russia to the central regions of the continent. Moreover, numerous nations have entered into long-term agreements with Russia, and during contract renewals the country often lowers its natural gas prices to retain its market dominance. As a result, Russia can influence political issues unrelated to energy because many European states depend on Russian gas without alternatives. Apart from the indirect effects of the Russia–Ukraine gas issue, there are no further concrete examples of Russia using gas as a political instrument against any EU member state (Rettig & Eran, 2018, pp. 105–106).

Ukraine is one of the primary transit countries for Russian gas exports to Europe, with Belarus in the second spot. It handles around five major Russian pipelines to Europe. Therefore, Ukraine is vital in the European energy landscape. However, over the years, Russia has tried to bypass Ukraine by sending gas to Europe through other pipelines, for instance, the Blue Stream, Nord Stream, and Turk Stream. Russia also completed the Nord Stream-II pipelines to export gas directly to Germany. Berlin viewed Russia as a reliable supplier if it were not for its need to transit through Ukraine due to the declining supply of gas from the North Sea. Germany pushed for this pipeline and resisted many calls by the US to stop constructing it. Moreover, Germany successfully persuaded the United States to impose limited sanctions on Russia to mitigate potential adverse effects on the project's viability. The president of the European Council, Donald Tusk, asserted that the pipeline will harm Europe's long-term interests due to its potential to heighten the continent's reliance on Russian gas. Several European Union member states, including Hungary and Poland, expressed significant dissatisfaction with Germany's endorsement of the pipeline project despite various cautionary indicators (Rettig & Eran, 2018, p. 105).

However, in response to the Russian attack on Ukraine, Germany had to decline the pipeline authorization. Later, in early September 2022, a section of the pipeline was severed in a sabotage act, with no one claiming responsibility. Since the conflict, the EU has paid Russia €35 billion for energy supplies, which is still a lot of money compared to the help it has provided Ukraine (Zerkal et al., 2022). Despite the dependency, experts warn that Europe's energy security is jeopardized, given the imposition of sanctions on Russia for its Ukrainian adventurism (McBride, 2022).

Russia–Europe Energy Confrontation

Russia uses its vast oil and gas reserves for commercial and political interests. Mike Pompeo, the US Secretary of State, described the Russian gas projects as "the Kremlin's key tools to exploit and expand European dependence on Russian energy supplies" (Ozawa & Iftimie, 2020, p. 13). The current disruption of Russia–Europe/Ukraine energy relations is not spontaneous. Given the previous episodes, it was already under strain. In 2006 and 2009, a major crisis was triggered in Europe due to differences between Russia and Ukraine over transit fees and gas pricing. Russia eventually stopped supply to Ukraine, resulting in supply disruption for Europe, which stretched for around two weeks. As a result of its actions, Russia lost its reputation and was seen as an unreliable supplier. European policymakers feared that Russia might, in the future, employ energy as a ransom for political leverage.

After Ukraine joined the Energy Community in 2011, Russia made serious attempts to wean off Ukraine from the EU's orbit. Russia's energy diplomacy became one of the prominent reasons for the 2014 Euromaidan protests in Ukraine. The Kremlin hard sold its energy card to compel the Ukrainian leadership to abandon EU integration plans. After the formation of the anti-Russia government in Ukraine in 2014, Russia cancelled the 2010 Kharkiv Accords, which gave Ukraine inexpensive gas in return for the lease of Sevastopol (Crimea) until 2042. Ukraine's energy ties with Russia were further strained by the loss of energy-rich regions to Moscow-supported separatists (Surwillo & Slakaityte, 2022, p. 2). The region's energy transit infrastructure was heavily damaged, jeopardizing the European energy supply. Alternatively, Moscow started constructing other pipelines (Nord Stream) to bypass Ukraine and directly link up with the EU market. The loss of transit routes for Ukraine was the primary reason for its objection to Russia's new energy pipelines. It feared that these pipelines would establish Russian leverage over Europe.

The confrontation can also be seen as an extension of Russia–US/NATO competitiveness in Europe. The US shale gas production, and its export to the European market, are viewed as challenging the Russian position as the primary supplier. Russia has powerfully conveyed its displeasure about NATO expansion. Hence, the Russian invasion of Ukraine is regarded as a signalling to other countries of its thresholds. Reportedly, friction has grown between the US and Russia over Arctic activities. There are broad disagreements over exploration rights and mitigating environmental consequences.

European Union Sanctions on Russia

Following the Russian attack on Ukraine, the EU imposed one of its harshest sanctions, especially on the Russian energy sector. The European Union has banned the import of crude oil and refined petroleum products from Russia. The oil embargo has had a significant effect on Russia. The country's dwindling budgetary reserves are directly attributable to the loss of this leading lucrative market. Some 90% of the European Union's oil imports from Russia are affected

by the prohibition. Russia loses over €8 billion annually due to the import ban on Russian coal, which affects almost a fourth of its global coal exports. The G7+Price Cap Coalition's agreed-upon price restrictions have not only helped stabilize global energy markets but also cut Russia's income from oil. The price limitations prevent, for instance, EU operators from transporting Russian oil beyond the cap or providing insurance for such a shipment. As of now, there are three export price caps in place- a ceiling of $US47.6 per barrel has been set for Russian seaborne crude oil; $US100 per barrel has been set for: premium-to-crude: petroleum products like diesel, kerosene, and gasoline; and $US45 per barrel has been set for: discount-to-crude: petroleum products such as fuel oil and naphtha (EC, 2023). Other restrictions on the energy sector include:

- No import of Russian coal.
- No new EU investments in mining within Russia, except for specific raw materials.
- Export restrictions on refining technologies, making oil refinery upgrades more challenging and more expensive for Russia.
- Extensive embargo on new energy investment in Russia, including exceptions for civil nuclear energy and transporting certain items to the EU.
- Barring Russians from leasing EU gas storage capacity.
- Ban pipeline imports of Russian oil for Germany and Poland (EC, 2023).

Rationale Behind Russia's Energy Card

Russian Deputy Prime Minister Alexander Novak stated: "We have every right to take a matching decision and impose an embargo on gas pumping through the Nord Stream 1 gas pipeline." (Surwillo & Slakaityte, 2022). Russian authorities are aware that the European market is stagnant; they want to keep it going for as long as they can, but they know that the future of the country, in terms of economic expansion, revenue, and market, lies in places like China, India, Southeast Asia, and South America (Aspen Institute, 2019). According to Sergey Vakulenko, a non-resident fellow at the Carnegie Endowment for Peace, Russia has taken a "calculated application of pain and measured deployment of the economic warfare arsenal" (Vakulenko, 2022). Terminating the gas supply remains a potent weapon for Moscow, arguably more useful as a threat. Given the ongoing conflict, Russia has few options in the event of an escalation. Russia views the European turn towards renewables and the likelihood of US LNG entering the European market after 2025 as unfair, diminishing the value of Russia's energy trade with Europe.

Overall, Russia's use of energy cards in the current war is meant to solidify its influence and power over Ukraine and Europe, while also highlighting the need for energy diversification and increased energy security. Strategically, Russia sees Europe's reliance on its gas as giving it the power it needs to coerce European nations into accepting Russia's political demands about Ukraine in exchange for a relaxation of sanctions (Vakulenko, 2022). The Russia–Ukraine

war has wider repercussions for the energy market and is reshaping energy geopolitics in several ways. In a significant shift, serious efforts are being made to phase out EU–Russia energy cooperation. Their mutual dependence was under strain, but no one had calculated what the potential consequences of their breakup. European leaders are now faced with a tricky challenge to contain Russia, on the one hand, and to shield themselves from the resultant economic fallout, on the other.

Revenue from energy sales helps finance Russia's war, which European leaders want to cripple by banning the country's energy imports. However, in doing so, they are faced with soaring energy prices and high inflation. Experts have warned about the impending global recession hitting significant economies by 2023 (Hussain, 2022). EU, in its immediate actions to the 2022 invasion, instituted gradual punitive sanctions on Russia. Notably, it cut off ten major Russian financial firms from the SWIFT network while putting a complete ban on coal imports. In June 2022, the EU passed its sixth sanctions package, which banned seaborne crude oil and petroleum product imports from Russia. It also debarred EU shipping companies from offering maritime transport services for petroleum shipments from Russia. Later, the G7 states announced a price cap on Russian crude oil and refined products to prevent Russia from benefitting from high fuel prices and limiting revenue from energy exports. In October 2022, as part of the eighth sanctions package, the G7 countries agreed to put a $60/pb price cap, effective from 5 December 2022; the price cap for refined products went into force on 5 February 2023.

Several global energy firms have either pulled out of Russia entirely or significantly reduced their operations there. They have frozen fresh investments and begun to sell off their Russian holdings. Consequently, Russian exports to Asia have drastically risen since February 2022, while European imports have significantly dropped (EIA, 2023b, pp. 1–2). There is churning in the international energy market, and supply disruption has led to a global economic slowdown. Households and companies are feeling the effects of high and fluctuating energy costs, causing people to utilize other fuels. The soaring fuel prices, decreasing income, and rising prices have all contributed to an impending global recession. IEA attributes rising fuel costs as the reason for the 90% rise in global electricity generation costs (Thomson, 2022). Reportedly, Germany incurred a loss of 12% in its GDP because of an increase in energy prices. Following the spike in domestic electricity and gas charges in the UK, inflation is expected to rise to 13%. Europe has been suffering from an all-time high wholesale electricity price since 1999 (Pollitt, 2022). There is destabilization in energy consumption and production. Irrespective of the Asian demand, the supply disruption to Europe, compounded by a slump in US shale production, has created severe energy deficiency in Europe. During the initial days of the Russian attack, European gas prices alarmingly rose to around 580%, but were later stabilized only under the Russian-approved payment procedure.

The export payment was routed through a non-sanctioned Russian bank, facilitating rouble payments to Gazprom (Thompson, 2022). Coal and oil

import bans in Europe and gas cuts by Gazprom are causing a significant shift in global trade patterns. Russian exports to Asia have seen a sharp increase and the country had already had initiated plans for diversification of its market. The Russian government's *Energy Strategy for 2035 has* already strategized to "diversify energy exports," paying attention, "particularly in the Arctic region," while "prioritizing exports and revenue" (Sukhankin, 2020). From January to October 2022, Russia transferred 1.4 tcf of natural gas to Europe, a significant drop from 2.9 tcf sent in the same period in 2021. Comparatively, in the same January–October 2022 cycle, Russian gas exports to China increased via the *Power of Siberia* pipeline. In the same intervening period (January–October 2022), Russia exported 2.1 bcf of LNG to Japan, China, and France (EIA, 2023a, pp. 12–13). Alternatively, Russia is providing a heavy discount on its energy exports to Asia and also some African countries to maintain its energy revenue. Moscow had already devised ways to circumvent the dependence on Ukraine for energy transit, through, for instance, the construction of the Nord Stream pipelines. These measures have cushioned Russia to evade the punishing sanctions. Despite the decrease in gas production and exports, Gazprom's profits remain on an upward trend (Kardaś, 2022).

The war has consequently forced many European countries to alter their energy policy. The primary objective of the EU is not to diminish the influx of gas from Russia but rather to enhance its negotiating leverage by offering alternative gas sources. This approach aims to disassociate Russian gas from its political implications. However, despite the recent decline in prices, it is anticipated that importing LNG will be considerably more costly for European nations than importing gas via pipelines from Russia. Furthermore, it is worth noting that Eastern European countries also need more direct access to maritime routes. Consequently, these countries rely on their neighbouring nations to facilitate the transportation of gas using interconnected pipeline systems. This phenomenon leads to an increase in the cost of petrol. It necessitates enhancing current infrastructure links between the nations to accommodate the augmented volume of transported petrol (Rettig & Eran, 2018, pp. 106–108). There is a growing debate about switching to a renewable energy source. Although immediate actions have concentrated on ensuring supply and safeguarding customers, the European Union countries have implemented new laws that significantly increase expenditures in clean energy and efficiency. However, these new laws and measures initiated in extreme times will take time and may not provide instant relief. Hence, policymakers are contemplating coal-based sources and revamping nuclear energy production capacities. Simultaneously, the world's liquid fuel production and consumption balance does not appear to alter much in the backdrop of the Russia–Ukraine conflict (EIA, 2023b).

Conclusion

The February 2022 Russian invasion of Ukraine triggered a parallel war in the energy market, as Russia challenged Europe's dependence on its energy supplies. Western countries responded with punitive sanctions aimed at crippling

Russian power and finance. Europe, in turn, sought to reduce its reliance on Russian energy. However, Russia's position as a primary energy supplier and its control over oil and gas prices has allowed it to exert political leverage and maintain its influence. The chapter explored the geopolitical significance of energy, which is intertwined with international politics, security, and economic growth. Russia's abundant energy resources and distribution network have made it the primary supplier for Europe, giving it political leverage over the region. While Europe attempts to diversify its energy sources, the process remains challenging and time-consuming.

The conflict between Russia and Europe has also disrupted the energy supply and contributed to soaring fuel prices, leading to a global recession and inflation. European countries face the dilemma of countering Russia's actions while protecting themselves from economic fallout. Russia, on the other hand, is adapting its energy export strategy to maintain revenue and influence, focussing more on Asian markets. The war has forced European countries to rethink their energy policies, with increased emphasis on renewable energy sources and energy efficiency. However, these changes will take time to implement and may not provide immediate relief from the energy crisis caused by the conflict.

References

Aspen Institute. (2019). *A booming sector grappling with diversity, global instability, & climate change*. Washington, DC: Aspen Institute.

Dreyer, I., Stang, G., Mandil, C., & Henderson, J. (2014). *THE geopolitics of energy: EU foreign policy and global energy security*. Paris: European Union Institute for Security Studies.

Early, C., & Saush, A. (2022, March 10). *What does the war in Ukraine mean for energy security in Europe?* Retrieved from https://www.conference.board.org/topics/geopolitics/energy-security-europe-ukraine-war

EC. (2023). *EU solidarity with Ukraine: Sanctions on energy*. European Commission. Retrieved from https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine/sanctions-energy_en

Economist. (2018). https://www.economist.com/special-report/2018/03/15/clean-power-is-shaking-up-the-global-geopolitics-of-energy

EIA. (2023a, January 17). *Country analysis brief: Russia*. Washington, DC: US Energy Information Administration. Retrieved from https://www.eia.gov/international/analysis/country/RUS

EIA. (2023b, August 8). *Short-term energy outlook: Global oil markets*. Washington, DC: US Energy Information Administration. Retrieved from https://www.eia.gov/outlooks/steo/report/global_oil.ph

Hussain, M. (2022, September 26). *Geopolitics of energy of the war in Ukraine & national responses to energy crisis*. Retrieved from https://www.hindustantimes.com/ht-insight/international-affairs/geopolitics-of-energy-of-the-war-in-ukraine-national-responses-to-energy-crisis-101664182282722.html

IEA. (2022, March 21). *Energy Fact Sheet: Why does Russian oil and gas matter?* Retrieved from https://www.iea.org/articles/energy-fact-sheet-why-does-russian-oil-and-gas-matter

IEA. (2023, August 3). *Emergency response and energy security: Ensuring the uninterrupted availability of energy sources at an affordable price*. International Energy Agency. Retrieved from https://www.iea.org/about/emergency-response-and-energy-security

Kardaś, S. (2022). *Gazprom: Dip in production and exports, profits up*. Warszawa: Centre for Eastern Studies (OSW).

McBride, J. (2022, February 22). *Russia's energy role in Europe: What's at stake with the Ukraine crisis*. Retrieved from https://www.cfr.org/in-brief/russias-energy-role-europe-whats-stake-ukraine-crisis

OPEC. (2025, April 13). Demand for crude oil worldwide from 2005 to 2024, with a forecast for 2025 (in million barrels per day) [Graph]. *Statista*. Retrieved from https://www.statista.com/statistics/271823/global-crude-oil-demand/

Ozawa, M., & Iftimie, I. A. (2020). *Russia's energy policy: Dependence, networks, and special relationships*. Rome: NATO Defense College.

Parfitt, T. (2009, January 3). *Ukraine accused of stealing Russian gas as fuel flow declines*. Retrieved from The Guardian: https://www.theguardian.com/world/2009/jan/03/russia-ukraine-gas-supplies-gazprom

Pollitt, M. (2022, September 7). *CERRE on the energy crisis: The energy market in time of war*. Centre on Regulation in Europe CERRE). Retrieved from https://cerre.eu/news/cerre-on-the-energy-transition-the-energy-market-in-time-of-war/

Rettig, E., & Eran, O. (June 2018). *The EU's energy challenges, memorandum No. 175*. Tel Aviv: The Institute of National Security Studies.

Rossbach, N. H. (2018). *The geopolitics of Russian energy: Gas, oil and the energy security of tomorrow*. Swedish Defence Research Agency.

Shaffer, B. (2009). *Energy politics*. Philadelphia: University of Pennsylvania Press.

Skeet, I. (1996). *Geopolitics of energy*.14th Ceri International Oil and Gas Markets Conference (pp 265–272). Calgary: Energy Exploration & Exploitation, 1996, Vol. 14, No. 3/4, Sage Publications Ltd.

Sukhankin, S. (2020). Russia's energy strategy 2035: A breakthrough or another impasse? *Eurasia Daily Monitor*, 17(78). https://jamestown.org/program/russias-energy-strategy-2035-a-breakthrough-or-another-impasse/

Surwillo, I., & Slakaityte, V. (2022). *With energy at play in the Ukraine war, everybody pays*.Danish Institute for International Studies.

Thompson, H. (2022, May 26). *What does the war in Ukraine mean for the geopolitics of energy prices?* Economic Observatory. Retrieved from https://www.economicsobservatory.com/what-does-the-war-in-ukraine-mean-for-the-geopolitics-of-energy-prices

Thomson, E. (2022, November 08). *6 Ways Russia's invasion of Ukraine has reshaped the energy world*. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2022/11/russia-ukraine-invasion-global-energy-crisis/

Tsafos, N. (2018). *Who's afraid of Russian gas?: Bridging the transatlantic divide*. Washington, DC: Center for Strategic and International Studies.

Vakulenko, S. (2022, July 27). *What are the Kremlin's calculations in its gas war with Europe?* Retrieved from https://carnegieendowment.org/politika/87579

Zerkal, O., Lee, J., Chow, E., & Sherr, J. (2022). *What does the war in Ukraine mean for Europe's dependence on Russian oil and gas? War on Ukraine: The geopolitics of energy*. London: Royal Institute of International Affairs.

Part III
Warfare and Geopolitics

12 Artificial Intelligence

A Paradigm Shift in Modern Warfare

Sandeep Tripathi, Sanjay Soi and Gusti Aju Dewi

Introduction

In the cognitive age, artificial intelligence (AI) is one of the most defining technological developments of the 21st century and the technological revolution triggered by AI will bring about a profound change in human interactions (Fricke, 2020). Knowingly or unknowingly, we are part and parcel of the general use of AI. In an interview, Laurent Alexandre gave the following interpretation of AI:

> A combination of vast databases, increasingly powerful computers and machine-learning algorithms, produced mainly by the American and Chinese digital giants, has accelerated the progression of artificial intelligence at a speed that's surprised even its promoters, the heads of Google, Apple, Amazon, Facebook, Microsoft and IBM. Google and Facebook, in particular, didn't see it coming. The first industrial revolutions were a challenge to our bodies, while AI focuses on our minds.
>
> (Alexandre and Miailhe, 2017)

Technology becomes a game-changer in both the economic and the defense sectors (Horowitz, 2018). The power of AI was displayed in 2016, when the best human player of the ancient Chinese game *Go* was defeated by the AI program Alpha Go. Mastery of *Go* requires a lifetime; however, the quality of AI program was such that it continued to improve by playing against itself. Therefore, within just a few years, it mastered the technique of playing the game. In view of the huge success of Alpha Go, the AI program, the whole world suddenly took notice of the power of AI. South Korea announced an investment of nearly US$1 billion for research and development of AI by public–private participation. China also took note of the power of AI and focused on development of AI not only for individual weapon platforms but also development of command-and-control decision-making capability (Mayer, 2018).

The main cyber and AI players today are the United States, Russia, China, and, to a lesser extent, the European Union (EU). Large tech companies, however, are mainly located in the United States and China, while Russia is

DOI: 10.4324/9781003633204-15

primarily focused on military and government efforts. Technologically, the EU lags behind them all (Zillner, 2019). The qualitative analysis has been employed to understand the extent to which AI can re-order international power hierarchies. AI is going to play a pivotal role as an enabling capability. "Many actors will face increasing temptation to delegate greater levels of authority to a machine, or else face defeat," noting that Russian authorities have "approved an aggressive plan that would have 30% of Russian combat power consist of entirely remote-controlled and autonomous robotic platforms by 2030." New technologies can influence the way a nation fights and wins wars. Another aspect that must be considered is the fact that different actors may be seen to apply the same technology in different ways. Currently, many analysts have declared that AI will have a large and possibly deterministic effect on global politics (Horowitz, 2018). McKinsey Global Survey confirms the explosive growth of generative AI (gen AI) tools. The study considered 2023 as the break out year for generative AI. AI was no longer limited to technical employees; it was a hot topic of top leaders in company in their board rooms. Companies were willing to enhance budgets for the development and incorporation of AI in their business.

Paradigm Shift in Warfare: Shaping Global Landscape

AI has emerged as a strategic game-changer in the landscape of evolving geopolitics. The world grapples with the rising role of AI on everyday life. The global landscape is being shaped by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT). Artificial intelligence transforms decision-making processes, facilitates citizen participation, and redefines global power dynamics (Tariq, 2024). An AI-capable nation-state has the potential to form new narratives, destabilize adversaries, and shape global perceptions. These accelerating technological advancements have significantly transformed the information warfare landscape in the 20th century. Radio and television had emerged as avenues for disseminating information during World War II. It was extensively used for propaganda purposes, illustrating the potency of information as a weapon. AI has now emerged as a powerful tool, reshaping the nature of propaganda and disinformation campaigns. It also plays a pivotal role in the creation of a wide range of content, from articles and images to entire news stories.

AI-powered cognitive warfare leverages disinformation to manipulate public perception, degrading trust in institutions and destabilizing societies. By automating digital large-scale influence operations, AI empowers hostile actors to customized deceptive narratives, amplifying psychological manipulation in hitherto unprecedented ways. Additionally, AI presents a dual-use dilemma; it can serve as a life-saving tool in fields such as accurate medical diagnostics, detecting diseases with high speed, yet in the wrong hands, it can be weaponized for autonomous warfare, cyberattacks, and massive disinformation campaigns.

The Cold War era saw the intensification of information warfare between the United States and the Soviet Union. Both superpowers engaged in a battle of ideologies, utilizing various media outlets to influence global perceptions. The Cuban Missile Crisis of 1962 highlighted the strategic importance of information dissemination, as both nations sought to control the narrative surrounding the event. The rise of the internet in the late 20th century represented a paradigm shift in information warfare. With the ability to rapidly share information globally, cyberspace became a new battleground. The Gulf War of 1991 demonstrated the use of advanced communication technologies, such as satellite imagery and 24-hour news cycles, to shape public opinion and control the narrative of the conflict. In the ever-evolving landscape of information warfare, this capability allows malicious actors to flood the information ecosystem with tailored narratives designed to influence public opinion. AI-generated content is not confined to textual information; it extends to the visual domain, where algorithms can generate realistic images that may accompany fabricated stories.

AI's involvement in the propagation of misinformation is deep and profound. In the era of digital connectivity, information warfare encompasses a wide range of activities, including the dissemination of propaganda, the manipulation of public opinion, and the use of cyber capabilities to disrupt and influence adversaries. The fusion of traditional military strategies with advanced technological tools has given rise to a new paradigm where battles are fought not only on the physical battlefield but also in the virtual realm. The Ukraine War, a significant and complex conflict that unfolded in the early 21st century, serves as a compelling case study for understanding the intricate interplay between traditional warfare and information warfare. The war has been characterized by a multifaceted information landscape, where the manipulation of narratives and the use of propaganda have played a pivotal role in shaping perceptions, both domestically and internationally (Pomerantsev, 2019). As we delve into the dynamics of information warfare in the context of the Ukraine War, it is essential to recognize the transformative impact of AI on modern conflicts.

We have noticed that, at present, generative AI is becoming part and parcel of every walk of life.[1] The superpowers are nervous about the growing supremacy of generative AI. The governments and the armed forces need to keep pace with these developments in order to maintain security and a technological edge. In future, dominance of a country may be decided not by the size of its armed forces, but by how efficient they are due to the use of AI and also how they are planning to use AI in future. Natural Language Procession (NLP) enables humans to communicate with machines using typical grammar and text rather than inputting codes. This has helped in the integration of AI tools in all walks of life; even a normal non-technical soldier can use the AI tool. The new development in AI is the advent of multimodal artificial intelligence. These systems can understand and respond to inputs in the forms of text, images, and a combination of audio and video. This means that humans can interact with machines or AI tools in a similar way to how they interact with

other human beings. This, on the one hand, is like a force multiplier; on the other hand, it makes it very challenging for security forces since all types of players can use these extremely advanced systems (Szabadföldi, 2021).

The Internet of Things (IoT) presents multiple entry points for attackers. Increased automation and machine autonomy in everyday life itself represents a strategic vulnerability. Nevertheless, there are visible changes that can be felt on a global scale. AI has made incredible progress, resulting in highly capable software and advanced autonomous machines. Meanwhile, the cyber domain has become a battleground for access, influence, security and control. The strategic implications of these parallel developments will be profound, particularly when used in combination. Military operations is more than just fighting on the front. It involves training, communications, automation, engineering, fire support defence and attacking elements in addition to transportations, logistics, repairs and medical services. AI can assist in all of the functions in terms of speeding up, and improving delivery. Operations means the usage of different types of systems, such as communications, detection, observation, analysis and deduction, can be carried out much faster and more accurately through the use of AI tools. This will also help to save manpower, which can be utilized for the principal operational tasks (Butun et al., 2020).

The intelligence build up is one of the major factors in determining the fate of the operations. Before and during operations, a huge amount of data from different sources is collected. These sources could include intelligence agencies, satellite pictures, images sent by the air force, drones, foot patrols and social media. Processing such a huge amount of data in a short time is a big challenge. AI assists through the collating data to come to a logical deduction. Wartime situations are very dynamic and the exploitation of opportunities offered during very short windows can tilt the outcome of the battle. AI can provide much faster processing of pictures, maps and reports from open sources. Similarly, NLP allows users to query the program and seek additional inputs. As a result, the level of productivity and accuracy achieved is much higher. The capability of AI even to predict the response by the enemy and to combine the operational plan with, for example, real-time weather reports, makes it a formidable force multiplier. Thereafter the information is disseminated to the concerned commander, who is able to take immediate action. This could involve the air force, air defence, ground forces or other logistic elements. In the present scenario, the amount of data which need to be analysed is almost impossible for human beings to comprehend, let alone process. AI also assists commanders to analyse data without any human prejudices. Hence, one is able to adopt the best course of action in shortest possible time. Both the Russia–Ukraine war and the Israel–Gaza conflict have illustrated the extensive use of AI (Fazekas, 2021). We have noticed how the Russian logistics convoys were attacked with precision and their commander killed. Israel also was able to inflict causalities on the leadership of Hamas with pin-point precision due to their use of AI. Most of the commanders and soldiers involved do not have technical background. NLP enables, non-technical personnel to communicate

with the AI tools, which is a big breakthrough. The user-friendly feature nature of AI helps in more rapid, direct communication between the commander with the AI tool. No middlemen or technical personnel is required to assist the commander, who can therefore focus on operational planning. Preparation for the war is a continuous process and training is an integral part of the preparedness of the armed forces. This is very well enunciated by US General Norman Schwarzkopf, who led Operation Desert Storm in 1991 against Iraq: "The more you sweat during peace, less you bleed in war." Present-day wars will be fought on different fronts and will not be restricted solely to the battleground. Therefore, any training also has to align to such contemporary circumstances. The war exercises are planned and conducted on the ground as well as on models and simulators. Pictures are created to give the actual feel of the battle. The construction of simulators requires a combination of engineering, software and a knowledge of hardware. NLP enables the interaction of AI with students and can assist in the preparation of content. Of course, human intervention is still necessary for the final evaluation.

Automation plays a major role in in day-to-day life, and crippling the systems will have a significant impact on both war-fighting capability and the will to fight. Military systems are generally not linked to outside networks, mainly as a result of security reasons. However, even these are vulnerable to cyber-attacks. What is taking place is actually a war within a war. The enemy would use AI to penetrate the system; defender would use AI to protect itself. In both cases, the technology works to find the gaps, predict the pattern, and attack or defend it (depending on the role). The loopholes need to be taken care of with regular updates based on updated threat perceptions. In recent years, drones have proved to be very effective since they have a very small radar signature and they are able to perform multiple tasks, depending upon the type of drone being used. AI is now being used to coordinate and launch drone swarms.[2] These swarms are much more effective than a singular drone. The areas covered can be very large and once any of the drones detects any suspicious movement, the other drones are informed and a coordinated action is planned. Another development is a more autonomous firing system; however, the use of such autonomous systems has serious ethical issues (Petrovski and Radovanović, 2022).

AI and Cyber Security

Future wars will not be fought solely on the battlefield. All spheres and sectors, from space to cyber, will be used to cripple the war-waging capabilities of the adversary. With the increase in automation and the development of the Internet of Things, the risk of cyber-attacks has increased dramatically. Hence there is a need to possess very powerful proactive as well as defensive cyber security measures. AI can assist in accelerating threat detection, response and decision-making. However, there is still a long way to go. There are also a number of challenges with using AI for cyber security. AI algorithms can be exploited

to manipulate data inputs. This can render the whole system redundant and result in inaccurate threat detections. Additionally, it is difficult to communicate using AI tools and there is no accountability in such a system. AI tools rely on the collection of huge amounts of data, which leads to privacy issues. In view of the fast-changing technology, tools also need to stay ahead to remain relevant. Hence, in the present scenario, AI can be used to assist humans; the final decision has to be rest with the commander on ground.

As we navigate the digital era of the 21st century, cyber security has grown into a pressing societal issue which requires innovative, cutting-edge solutions. In response to this pressing need, AI has emerged as a revolutionary instrument, causing a paradigm shift in cyber security. The use of this technology in the field of cyber security has been playing a vital role in vulnerability management, reshaping threat detection, and processing network security (Gruetzemacher & Whittlestone 2022). AI's prowess resides in its capacity to process and analyse immense quantities of heterogeneous cyber security data, thereby facilitating the efficient completion of crucial tasks. These duties, which include threat detection, asset prioritization, and vulnerability management, are performed with a level of speed and accuracy that far exceeds human capabilities, thereby transforming our approach to cyber security (Kumar et al., 2023).

AI and the War of Minds

We are living in an era characterized by digital hyper-connectivity and rapid technology advancement, and AI, with its deep learning algorithms and Neural Networks, have all significantly reconfigured the methods by which states conduct conflicts. Conventional battlefields have evolved and modern warfare increasingly targets the cognitive dimension, shaping public perception and morale through disinformation and digital psychological manipulation (Singer & Brooking, 2018). These concerning developments emerge as key components of hybrid warfare, blending traditional tactical operations with the strategic use of cognitive attack. Leveraging AI tools with destructive intention, such as Generative Pre-trained Transformer (GPT), a family of AI models that can generate human-like text, along with Deepfakes and automated social media bots, hostile actors can tailor content precisely for large-scale disinformation. These AI-powered tactics enable public opinion manipulation, disrupting political processes and even dividing nation and countries. These profound AI tools can have a serious impact; the user's intention will determine whether or not this will be constructive or destructive for the society.

Conceptual Framework: Disinformation, Psychological Warfare, and AI

Disinformation refers to the deliberate dissemination of false or misleading information intended to manipulate target audiences (Woolley & Howard, 2019). This differs from misinformation, which can also be inaccurate but is

distributed without the intention to deceive and manipulate. Psychological warfare (psywar), which involves broader tactics, including propaganda, intimidation and more subtle forms of influence, aims to weaken an adversary's morale and cohesion (Gartzke & Lindsay, 2019). Historically, psywar methods relied on print media, radio broadcasts and loudspeakers; modern developments draw heavily on AI-powered tools that can vastly extend their reach. This multiplies the psywar effects by automating message generation with the possibility of lower cost.

AI as a Force Multiplier

AI encompasses machine learning, deep learning, and natural language processing (NLP), all of which enable rapid, large-scale data processing (Cresci, 2020). In the disinformation campaign, AI can perfect content development and message targeting. Through the use of human-operated "troll farms", thousands of messages can be produced daily. AI systems, however, can generate and distribute even millions, customizing the personal tone and style to trigger specific emotional responses. AI analytics further identify psychological vulnerabilities, including social divisions or cultural tensions within targeted populations (Ferrara, 2017). So-called 'black campaigns' have the ability to deploy fear-mongering operations using precision-crafted narratives from big data. The integration of high-tech automation with behavioral insights enables bad actors to disrupt public trust and reshape societal discourse beyond previous scale expectations.

AI Tools and Techniques in Disinformation Campaigns: Automated Social Media Bots and Troll Farms

Social media has developed as a critical front in AI-powered disinformation. Automated accounts, or bots, pose as genuine users, posting polarized opinions, retweeting propaganda, and artificially inflating certain hashtags (Ferrara, 2017). Recent AI language models allow bots to mirror real human interactions more convincingly (Cresci, 2020). They have the ability to detect emotional triggers and vulnerability by analyzing trending topics in real time and engaging digital interaction to amplifying outrage and provoking viral spread. This orchestrated dangerous strategy can dramatically transform minor disputes into polarizing public arguments and drive entire digital communities toward antagonism. Chaotic social engineering powered by AI.

Deepfakes and Synthetic Media

Deepfakes, AI-generated or manipulated video and audio content, shows a more alarming threat. Created by techniques such as Generative Adversarial Networks (GANs), deepfakes can create political figures making incriminating

statements or performing actions that never happened (Mirsky & Lee, 2021). One striking example of this phenomenon unfolded following a heated meeting between US President Donald Trump and Ukrainian President Volodymyr Zelensky in March 2025. Their tense diplomatic exchange became a catalyst for a surge of AI-generated deepfake videos, including viral clips depicting Trump choking Zelensky and Zelensky punching Trump. Those digitally altered videos, widely circulated on social media, exemplify how AI-powered disinformation can fuel geopolitical tensions and disrupt diplomatic relations.

Even once clarified as a hoax, such content has already inflicted serious reputational damage that can turn into diplomatic turmoil because not everyone is willing to carry out the proper fact check before reacting; humans are emotional beings. The lingering uncertainty deepfakes create fosters what some analysts term the "Liar's Dividend": a scenario where any evidence, either genuine or artificial, can be dismissed as potentially forged (Li et al., 2020). Bad actors benefiting from this ambiguity, leveraging it to delegitimize valid accusations against themselves.

Micro-Targeting and Behavioral Profiling

AI, with all of its elements including NLP, Neural Networks, machine learning and deep learning algorithms, excels at classifying audiences to deliver micro-targeted psychological propaganda with a human strategist behind it. By profiling the user's behavior via digital activity, search histories or emotional responses, bad actors can tailor highly specific narratives that could engage the victim who shares everything about their life in cyber space personally. With bad intention, the narratives can contain fear-driven provocation to gain strong reactions from the intended target. This approach combines the use of data analytics, facilitated by AI algorithms, with nuanced awareness of social, cultural and psychological factors. As AI is continuously improving its model with new data, it slowly but surely adapts messaging in real time, driving more potent psychological influence than any "one size fits all" propaganda approach could achieve through the support of good data quality, strategic black campaign design and message credibility.

The Psychology of Influence in Modern Warfare

Cognitive Biases and Emotional Triggers

AI-driven disinformation frequently exploits well-documented cognitive biases, especially confirmation bias, which leads people to accept information that supports their preexisting views and to dismiss evidence to the contrary (Nickerson, 1998; Lewandowsky et al., 2012). All kind of emotional triggers, such as sadness, fear, anger or even ultra-nationalistic pride, emphasize social tensions among society and make communities more vulnerable to divisive

messages. Financial hardships, identity-based conflicts or controversial ongoing topics are among the main hooks for emotionally engaging narratives. By leveraging these, covert disinformation campaigns aim to intensify public anxiety, fear and grief, ultimately undermining trust in institutions and stifling rational discourse (Wardle and Derakhshan, 2017)

Strategic Manipulation of Narratives

The framing of the narrative is vital in psychological warfare. AI-powered analytics can do far more than we can imagine. With AI-driven analytics, the enemies can order the black actor to do cherry picking, select and highlight certain storylines with the purpose of dividing society or sowing doubts into the leadership. Campaigns might exploit historical disputes or peddle sensational conspiracies (Pomerantsev, 2019). The unifying theme is a simple "us vs them" narrative that results in polarization. AI's capacity to do large-scale data mining and sentiment analysis with NLP refines these tactics by processing millions of social media comments which spark the most emotional and strongest engagement and then create rapid manipulative narratives to maintain maximum impact. The majority of social media users, who do not understand these tactics, will buy into these narratives more readily. In particular, the result of AI-powered behavior manipulation can have a personal reach far beyond the static messaging of traditional war. Despite AI's capability to scale and speed, human expertise remains vital as the trainer behind the machine. Analysts conversant with data science, conflict studies and psychology can interpret AI-flagged content with meaningful contexts (Johnson, 2020). Human intervention remains vital to navigate and govern the misuse of AI for warfare.

Geopolitical Implications: Case Studies

Case Study 1 Election Interference

During the 2016 US Presidential Election, foreign actors, particularly from Russia, carried out coordinated disinformation campaigns using troll farms, bots and micro-targeted social media campaigning. These tactics exploited cultural and political rifts to heighten polarization and undermined trust in the electoral process (Jamieson, 2020). While data analytics and automated tools were employed, this effort did not rely heavily on advanced AI in the contemporary sense; rather, it showed how algorithmic targeting and digital psychological operations can manipulate political discourse on a large scale.

Case Study 2 Russia–Ukraine Conflict

Within the Russia–Ukraine war, Russian-linked troll and bot networks, documented by researchers such as Peter Pomerantsev (2019), have disseminated pro-Russian messaging while seeking to discredit Ukrainian leadership. These campaigns exploit historical grievances and nationalist sentiments to confuse international observers and unsettle domestic Ukrainian audiences. While most identified "fakes" involve mislabeled or edited footage, at least one high-profile deepfake surfaced in 2022, falsely depicting President Volodymyr Zelensky calling on Ukrainians to surrender. Such operations test Western capacity to detect and counter disinformation, reveal potential vulnerabilities in NATO intelligence and media verification, and aim to diminish Ukrainian morale. They also serve to bolster Russian domestic support for foreign policy actions.

Case Study 3 Southeast Asia Tensions

In Southeast Asia, disinformation campaigns, often relying on coordinated networks or semi-automated methods rather than purely advanced AI, exploit regional flashpoints such as the territorial disputes in the South China Sea. Local-language operations, including troll farms or automated "bot" accounts, can fuel inflammatory messages, stir nationalist sentiment, and deepen ethnic or political divides. These tactics may destabilize domestic politics and complicate diplomatic negotiation. Even partial truths, when repeated frequently, can erode trust

Countermeasures and Ethical Considerations

Detection and Verification Strategies

Fighting AI-driven disinformation will require layered detection systems. AI researchers have developed machine-learning algorithms that detect deepfake artifacts or "organized inauthentic behaviors on social media" (Li et al., 2020). As disinformation tactics evolve, however, an arms race emerges: new detection methods lead to more refined evasion by malicious actors (Cresci, 2020). Human-in-the-loop analysis bolsters automated screening. Well-trained analysts, familiar with regional context and nuanced socio-political cues, have the capacity to swiftly identify suspicious content. Fact-checking partnership, media literacy campaigns and strategic public awareness initiatives are still crucial components of an effective defense.

Media Literacy and Public Resilience

Media literacy stands as a critical front line against digital psychological warfare. By enhancing critical thinking skills, questioning sources, verifying evidence, aware and able to recognizing emotional manipulation, society become less vulnerable to deceptive narratives (van der Linden et al., 2017). Grassroots educational programs and digital toolkits help people to distinguish between fake and original content. This resilience-building approach typically requires multi-sector collaboration among government, agencies, NGOs, schools, universities and both traditional and modern media platforms. Even though such efforts might not give immediate results, they significantly mitigate the long-term impact of disinformation.

Strengthening an Integrated Strategic Role

Addressing AI-powered disinformation strongly demands multidisciplinary teams proficient in behavioral psychology, data analytics, and geopolitics (Johnson, 2020). By gathering these skill sets, governments, defense organizations, and think-tanks can interpret machine-generated insights with cultural empathy, bridging the gap between raw data and real-world social dynamics. The merging between AI-driven insights and human expertise results in more targeted countermeasures, be they rapid response units that counter viral hoaxes, public campaigns to protect citizens against manipulative content, or diplomatic engagements that mitigate regional disputes. Every strategy weaves predictive analytics with qualitative analysis, producing a holistic approach to information warfare.

Collaboration with Stakeholders

No single entity can handle AI-powered disinformation on its own. Military and intelligence services, tech companies, NGOs, academics, practitioners, and global institutions all hold unique capabilities and data resources. Organized intelligence sharing accelerates the detection of new tactics, while shared research drives the development of advanced, ethically guided AI solutions. Alliances, be they regional or global, can pool expertise to expose the circulation of disinformation that operates across multiple jurisdictions.

Conclusion

Artificial intelligence (AI) has redefined modern warfare, shifting the paradigm from physical confrontation to large-scale cognitive warfare deepfake manipulation and bots, executed in a highly structured and massive manner within cyberspace. Additionally, AI has enabled the development of autonomous lethal weapons, including highly sophisticated robotic systems, some as small and discreet as mechanized insect-like drones, capable of precision strikes and intelligence gathering. This poses significant challenges for national security, democratic stability, and international relations.

This paradigm shift raises urgent questions about ethical governance, human oversight and geopolitical stability. The accelerating AI race among global superpowers highlights a dangerous trajectory where strategic dominance may no longer be determined by traditional military capabilities but by the ability to wield AI in influence operations, autonomous combat and cyber warfare. AI-powered disinformation and digital psychological warfare are also intensifying the role of cognitive influence in global security. AI tools, such as automated bots, deepfakes, and micro-targeted propaganda campaigns, can undermine trust and divide societies at remarkable speed (Singer & Brooking, 2018). Confronting these dangers requires a comprehensive approach.

As was warned by Geoffrey Hinton, the Nobel Prize in Physics winner known for his work on artificial neural networks (AI that imitates human neurons), which earned him the title the "Godfather of AI", the potential of AI surpassing human control is no longer science fiction but an emerging reality. The risks posed by autonomous weapon systems, which could make 'life-or-death' decisions without human intervention, demand immediate international regulation and governance frameworks. This warning calls for a multi-stakeholder approach, bringing together government, the defense sector, AI researchers, ethicists, and civil society to ensure AI is developed and deployed responsibly. Only with clear ethical safeguards and legal frameworks can AI enhance global stability. The AI revolution in warfare is inevitable and its outcome depends on how leaders and societies navigate this critical moment in history.

Notes

1 AI is no more to use by technical people only. The strength of the AI tools is that these can be utilized by totally non-technical person.
2 The drone as a new area of military technology has changed dramatically with the use of artificial intelligence to create a new horizon of warfare.

References

Alexandre, L., & Miailhe, N. (2017). The geopolitics of AI and robotics. *The Journal of Field Actions*, 17, 84–87. https://journals.openedition.org/factsreports/4507?lang=en+%28+Alexandre%2C+2017%29

Butun, I., Osterberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks and countermeasures. *IEEE Communication Surveys and Tutorials*, 22(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364. https://www.researchgate.net/publication/337234306

Cresci, S. (2020). A decade of social bot detection. *Communications of the ACM*, *63*(10), 72–83. https://dl.acm.org/doi/10.1145/3409116

Fazekas, F. (2021). AI and military operations' planning. In *Artificial Intelligence and Its Contexts*, edited by Visvizi, A. & Bodziany, M. (pp. 79–91). *Advanced Sciences and Technologies for Security Applications*. Cham: Springer. https://doi.org/10.1007/978-3-030-88972-2_6

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, 22(8). https://www.semanticscholar.org/paper/Disinformation-and-Social-Bot-Operations-in-the-Run-Ferrara/7a6823d16a1dc680c9bdfe03dc4caccbe2e944b6

Fricke, B. (2020). Artificial intelligence, 5G and the future balance of power. *Konrad Adenauer Stiftung*. http://www.jstor.org/stable/resrep25281

Gartzke, E., & Lindsay, J. R. (2019). *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press. https://academic.oup.com/book/35252

Gruetzemacher, R., & Whittlestone, J. (2022). The transformative potential of artificial intelligence. *Futures*, 135, 102884. https://doi.org/10.1016/j.futures.2021.102884

Horowitz, M. C. (2018). *Artificial Intelligence, International Competition, and the Balance of Power*, 1(3), 36–57. https://doi.org/10.15781/T2639KP49

Jamieson, K. H. (2020). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*. Oxford University Press. https://www.researchgate.net/publication/333123451_Cyberwar_How_Russian_Hackers_and_Trolls_Helped_Elect_a_President-What_We_Don't_Can't_and_Do_Know

Johnson, A. (2020). *Behavioral Insights for Cybersecurity Strategy*. Routledge. https://www.routledge.com/Cybersecurity-for-Information-Professionals-Concepts-and-Applications/Chang-Hawamdeh/p/book/9780367506971?srsltid=AfmBOopJ-oiP2l5kem255cRsmWY-zhbPOcL3nlcfttnQCm72rv8-PyUg

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: Revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, 2(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Lewandowsky, S., Ecker, U. K., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, 13(3), 106–131. https://www.researchgate.net/publication/258180567_Misinformation_and_Its_Correction_Continued_Influence_and_Successful_Debiasing

Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2020). Celeb-DF: A large-scale challenging dataset for deepfake forensics. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 3207–3216). https://arxiv.org/abs/1909.12962

Mayer, M. (2018). Artificial intelligence and cyber power from a strategic perspective. *IFS Insights*. 4/2018. https://core.ac.uk/download/pdf/225935404.pdf

Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR)*, 54(1), 1–41. https://dl.acm.org/doi/10.1145/3425780

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2), 175–220. https://psycnet.apa.org/record/2018-70006-003

Petrovski, A., & Radovanović, M. (2022). *Application of Drones with Artificial Intelligence for Military Purposes*. https://www.researchgate.net/publication/364324778_

Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War against Reality*. Faber & Faber. https://www.academia.edu/121290051/This_is_Not_Propaganda_Adventures_in_the_War_Against_Reality

Singer, P. W., & Brooking, E. T. (2018). *Likewar: The Weaponization of Social Media*. Houghton Mifflin Harcourt. https://www.researchgate.net/publication/335149861_Like_War_-_The_Weaponization_of_Social_Media_by_P_W_Singer_and_Emerson_T_Brooking

Szabadföldi, I. (2021). Artificial intelligence in military application – opportunities and challenges. *Land Forces Academy Review*, 26(2), 157–165. https://doi.org/10.2478/raft-2021-0022

Tariq, M. U. (2024). The role of Emerging Technologies in shaping the global digital government landscape. *Emerging Developments and Technologies in Digital Government*, 160–180. https://doi.org/10.4018/979-8-3693-2363-2.ch009

Van der Linden, S., Roozenbeek, J., & Compton, J. (2017). Inoculating against fake news about COVID-19. *Frontiers in Psychology*, 8, 566790. https://www.researchgate.net/publication/344831630_Inoculating_Against_Fake_News_About_COVID-19

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. *Council of Europe*. https://www.researchgate.net/publication/339031969_INFORMATION_DISORDER_Toward_an_interdisciplinary_framework_for_research_and_policy_making_Information_Disorder_Toward_an_interdisciplinary_framework_for_research_and_policymaking

Woolley, S. C., & Howard, P. N. (2019). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press. https://www.oii.ox.ac.uk/research/publications/computational-propaganda-political-parties-politicians-and-political-manipulation-on-social-media-2/

Zillner, M. (2019). Why is Europe lagging behind in the tech race? *European Generation*. https://www.europeangeneration.eu/single-post/2019/02/14/

13 The Dynamics of New-Generation Warfare Methods and Arms Exports in the Contemporary World Order

Chakali Bramhayya

Introduction

In the context of the development of global security, tremendous changes have occurred in the landscape of new-generation warfare (NGW) methods. NGW methods are a mix of disinformation campaigns, economic coercion, artificial intelligence (AI), and cyberwarfare, and these have been playing a predominant role in the conflicts of the 21st century. Arms exports and imports have become key factors in foreign policies. Major powers have been transferring technology to other countries to play an active role in contemporary global politics. This chapter critically examines the correlation between the global arms trade and NGW methods. Further, it will critically elucidate the repercussions of the NGW methods and arms exports for global power dynamics and global security.

New-generation warfare methods have been different from traditional battlefield methods, including the weaponization of non-military tools, hybrid warfare, and asymmetric strategies. Information warfare, AI-driven combat systems, cyber-attacks, and proxy conflicts have played detrimental roles in the military doctrines of the contemporary world order. Arms exports and imports have played a significant role in contemporary global politics. The defence industries are playing a pivotal role and have become powerful actors in facilitating the countries to develop dynamic foreign policy, strategic partnership and defence cooperation. Russia, the United States and China have been dominating global arms exports and exporting modernized weapons to various developing countries and the developed world. Finally, it is leading to the development of regional conflicts worldwide. Countries in South Asia and West Asia have been spending heavily on defence expenditure and arms imports.

Hypersonic cruise missiles, advanced capabilities, and modernized AI-based drone technology have altered the balance of power in the various regions and accelerated regional conflicts. Recent developments in the trilateral security partnership between Australia, the United States, and the United Kingdom in the Indo-Pacific region and the development of Russia–China strategic defence cooperation have brought about dynamic changes in global security. Various legal and ethical aspects are involved, with special reference to the methods of

DOI: 10.4324/9781003633204-16

warfare and arms proliferation in the new generation. Since there are no international mechanisms and regulations about AI-driven military technology and cyber warfare, this will lead to the proliferation of regional conflicts. The development and manufacturing of surveillance tools, military technology, and advanced lethal weapons will complicate the governance frameworks in the contemporary global world. Weapons have always been exported as a tool of influence and coercion. This is now leading to the violation of human rights and exacerbating the global security dilemmas in the contemporary world order.

The significance of NGW methods will increase in the contemporary multipolar world order. They will play a significant role in shaping global arms conflicts. Cooperative security frameworks, international regulations, and cyber-defence frameworks are required to regulate the guidelines related to new-generation warfare methods and arms proliferation. AI will play a significant role in emerging defence technologies, arms exports, regional stability, and military strategies. Russia has designed its military policy in the contemporary global world to emphasize new-generation combat techniques. It includes both traditional and modern approaches to dealing with various security threats in the uncertain global world. This chapter will critically elucidate the latest developments in Russia's military strategy and global arms exports. Russia is employing asymmetric and traditional military strategies in new-generation warfare strategies. Russia has used hybrid warfare strategies, cyber warfare, proxy troops, and disinformation campaigns. Information operations have been playing a predominant role in weakening enemies and influencing attitudes through manipulating propaganda and social media. Recently, Russia has developed new technology in precision strike capabilities, which have achieved the objective of attacking identified operations with high accuracy and minimum damage.

Highly advanced electronic warfare systems have been targeting the communications and radar systems of enemy camps, which, in turn, has increased the military offensive capabilities of Russia. Surveillance capabilities have been integrated with unmanned systems. These developments allow Russia to play a pivotal role in the global arms market and to expand its strategic cooperation with India and China. Southeast Asia, the Middle East, and Africa have imported defence equipment from Russia. In this connection, this chapter will critically analyse the latest trends of Russia's NGW methods and arms exports to global countries in the contemporary world order.

Contemporary Trends in the Dynamics of New-Generation Warfare Methods and Arms Exports in the Contemporary World Order

NGW approaches have played a vital role in modern military techniques. Autonomous weapons, cyber operations, AI, and hybrid tactics are the characteristics of the new generation of warfare methods. Weapon imports and exports have shaped the dynamics of global security. Traditional warfare methods, i.e., warfare with economic pressure, disinformation campaigns, and cyber

operations, give rise to new-generation warfare (Galeotti, 2019a). New warfare methods focus on asymmetric strategies and exploit digital, political, and economic weaknesses. The emergence of cyber warfare is one of the key elements of the NGW approach (Singer & Brooking, 2018).

Warfare in the New Generation: A Technological and Hybrid Development. The Role of Artificial Intelligence and Autonomous Systems

Autonomous systems and weapons driven by AI are revolutionizing warfare. Drones/Unmanned Aerial Vehicles (UAVs) have been most effective in recent conflicts such as the Libyan, Syrian, and Nagorno-Karabakh wars (Schneider, 2020). AI has increased battlefield surveillance and predictive analytics and reduced human involvement in combat scenarios. AI-driven technology has profound implications with regard to escalation risks and accountability (Boulanin & Verbruggen, 2017).

Hybrid Warfare and Non-State Actors

Hybrid warfare includes a blend of economic, psychological and military operations to deal with the adversaries. The strategy of Russia in Ukraine and Crimea has demonstrated that employing cyber-attacks, using irregular forces and economic pressure to the strategic objectives (Galeotti, 2019b). Non-state actors, i.e. insurgent groups and terrorist organizations, have exploited the hybrid tactics. ISIS, for example, has utilized the social media platform for propaganda, psychological warfare, and recruitment (Winter, 2018). Non-state actors have been using modernized drones; secured communication has increased their strategies in asymmetric conflicts. (i) Arms Exports, Leading to Strategic Leverage and Geopolitical Influence: Arms exports have predominantly determined the global security environment. Major arms-exporting countries, i.e., Russia, European nations, China, and the United States, have been using arms sales to strengthen bilateral relations and relations with multilateral institutions and gain economic benefits (Bitzinger, 2021). (ii) The Rise of Emerging Arms Exporters: Global arms exporters, i.e., Russia and the USA, have dominated the global arms market. Contemporary emerging players, i.e., South Korea, Turkey, and Israel, are becoming increasingly prominent due to their advanced defence technology and weapons manufacturing. For example, Bayraktar TB2 drones from Turkey were extensively used in the case of the Caucasus, Ukraine (Kırdemir, 2022).Similarly, South Korea has increased its defence exports with special reference to missile systems and developed strategic partnerships with Asia and other countries (Wezeman et al., 2023a). (iii) Arms Sales and Proxy Conflicts: Arms exports have increased immensely, contributing to various proxy conflicts. Major global arms exporters have transferred military weapons and equipment rather than facing direct military interaction. This has been witnessed in the conflicts of Syria and Yemen, where

Russia, Saudi Arabia, the US, and Iran have been supplying military equipment to different factions. It is therefore leading to the exacerbation of conflicts and the spread of instability (Bapat, 2012). (iv) Regulation and Ethical Concerns: The Arms Trade Treaty (ATT) has been unable to regulate arms exports, and it has remained a big challenge. Many countries are prioritizing strategic and economic interests over ethical considerations. Arms have been supplied to those countries with poor human development index and human rights records (Garcia, 2019)Africa and the Middle East are becoming more unstable as a result of the development of arms with light, lethal weapons and high power, which are responsible for the exacerbation of the conflicts in the areas (Marsh, 2021).

(v) The Relationship between Arms Exports and NGW: Global security and military strategies have changed as a result of the integration of new-generation warfare methods and arms exports. Countries have invested heavily in AI-driven defence technology, autonomous weapons, and cyber capabilities. (vi) The Digitalization of Warfare Trade: Digital surveillance tools and cyber weapons are important commodities in the arms trade. Private companies have been selling hacking tools, spyware, and cyber espionage capabilities to clients and allies across the globe. The Pegasus spyware crisis has revealed the involvement of global trade in digital technologies. It has also raised questions about cyber espionage and human rights violations (Feldstein, 2020). (vii) Drone Proliferation and Asymmetric Threats: The nature of warfare has changed as a result of drones being accessible. Countries acquiring UAV technology use it for reconnaissance, targeted strikes, and electronic warfare.

The use of Turkish and Iranian drones in regional conflicts demonstrates how drone proliferation enhances asymmetric capabilities (Kırdemir, 2022). Non-state actors have also acquired drone technology, posing new security threats to state militaries and civilian populations. (viii) AI and Military Export Controls: Countries have faced numerous challenges ever since AI technologies have driven military applications and technologies, and have become involved in regulating AI exports. The software of Artificial Intelligence can be transferred digitally. The United States and its allies have implemented various export control mechanisms on AI technologies to stop the difficulties of gaining military technologies **(**Horowitz, 2019). In this context, Russia and China have been continuously developing AI-driven military export systems, ultimately contributing to the AI arms race.

New Warfare Strategies in the Contemporary Global World

Russia has used advanced military equipment and innovative military tactics in Eastern Ukraine and Crimea. Western scholars have developed new theories to analyse Russia's new warfare methods. Russia has employed the techniques of the Gerasimov Doctrine: grey zone combat, hybrid threat, non-linear warfare, fourth-generation warfare, and hybrid warfare. Western scholars and theoretical frameworks have analysed the Russian new warfare methods from their

perspective (Bērziņš, 2020). Russia has defined the objectives of "sub-threshold warfare" (Bērziņš, 2020). Russia adopted a multifaceted and complex strategy to analyse the scenario in Ukraine and Syria. Russia has developed new warfare methods, military strategies, and various innovative methods from its own experiences and narratives (Bērziņš, 2020). There have been several narratives and reinterpretations of the new warfare method, i.e., hybrid warfare. Hybrid wars have been playing a vital role in uniting both irregular and regular forces on the battlefield. After Russia annexed Crimea and military intervention in Eastern Ukraine, western scholars have redefined the concept of hybrid warfare (Muradov, 2022). Russia and the West have different narratives with regard to hybrid warfare methods. Russia will not accept the argument that it was the victim of the hybrid warfare of the West. Russia's concept of hybrid warfare may apply to the examples of Ukraine and Georgia. Russia has been employing the technique of hybrid warfare to limit the ability of republics of the former Soviet Union in contemporary global politics (Muradov, 2022).

Hybrid warfare has gained a great deal of momentum ever since Russia annexed Crimea and Russia's policies in eastern Ukraine in 2014. There is a divergence of opinion about Russia's hybrid warfare objectives. Some scholars have argued that Russia's actions are very effective in the case of Eastern Ukraine, whereas other scholars have different opinions about their operations (Fabian, 2019). The concept of hybrid warfare in Russia is more than that of Western myth. It has the basis of the Gerasimov doctrine and historical factors. Russia has frequently used cyberspace and cyber technology in recent conflicts (Fabian, 2019). The West has developed a different perspective after Russia's military intervention in Ukraine with regard to hybrid methods of a "new way of war," i.e., militias, intelligence, special troops, coordinated use of criminals, and media operations (Galeotti, 2016a). Most of these tactics are the origin of Soviet and Soviet Russian practices. During Soviet times, Russia segregated non-state actor integration, military command structures and political command strictures.

Modern conflicts have emerged according to the prevailing technological, military, social environment, and political and military factors (Galeotti, 2016b). Russian actions in Crimea and Eastern Ukraine surprised many in the West by utilizing well-known military tactics in novel ways and with the aid of cutting-edge technologies. Western analysts immediately started looking for descriptions of this "new" approach, most of which were found within the West's theoretical framework (Bērziņš, 2020). They have included fourth-generation warfare, the Gerasimov Doctrine, hybrid warfare and hybrid threat, non-linear warfare, and, most recently, "*grey zone*" combat. However, many Russian theoretical discussions regarding novel combat tactics have not received sufficient attention. Due to this, Russian strategy has been characterized incorrectly, as it has been altered to suit Western theoretical frameworks rather than the ones in which it was initially formed (Bērziņš, 2020).

Since none of the above categories accurately capture Russia's ideology or presumptions about the nature of war in the 21st century, they have tended to be

useless rather than aiding in evaluating the options available to Russia (Bērziņš, 2020). The primary goal of this essay is to explain Russian "sub-threshold warfare", as Russia defines it. Almost 30 years' worth of Russian military literature, case studies from Crimea and Eastern Ukraine constructed from conversations with Ukrainian military and security professionals, and data on the Syrian situation derived from Russian sources were all used to analyse this scenario. The Russian military has a complex and multifaceted strategy, as evidenced by examining its military literature and an empirical review of its actions in Syria and Ukraine. Framing the Russian strategy regarding hybrid warfare or other artificial constructs created outside the context of danger is ineffective. Though it draws inspiration from Western military doctrine, the Russian framework is the product of their theoretical developments (Bērziņš, 2020). Russia's recent actions in Ukraine have raised concerns in the West about a "new way of war," frequently referred to as "hybrid," notably about the coordinated use of criminals, militias, media operations, intelligence, and special troops (Galeotti, 2016a). However, besides being recognizable from Western operations, many tactics also originate in Soviet and pre-Soviet Russian practice. Their willingness to prioritize "non-kinetic" measures, the extent of non-state actor integration, and the close ties between military and political command structures set them apart.

All of this, however, mostly comes down to degree rather than actual qualitative originality (Galeotti, 2016b).

Elements of Russia's New-Generation Warfare

i **Political Subversion**: The following aspects are included as part of political subversion: Traditional "*agit-prop*" information operations and the insertion of agents have taken advantage of linguistic, class, and ethnic divides through the use of intimidation of local authorities, compromise, mass media, corruption facilitated by assassination, terrorism, and dissatisfied elements (Phillip, 2015).

ii **Proxy Sanctuary**: The act of seizing police stations, military depots, local government buildings, and airports, developing checkposts, demolishing transport infrastructure, establishing the People's Republic under the guidance of Russia and conducting a referendum with the political party, which has already been represented in the political system (Phillip, 2015).

iii **Intervention**: Intervention methods include rigorous drills involving airborne forces, naval, air and ground forces, the establishment of training camps, and the transfer of heavy weapons to rebels (Phillip, 2015). The deployment of Russian forces to the border included abrupt, extensive drills involving air, ground, naval, and airborne forces; the covert transfer of heavy weaponry to rebels; the establishment of training and logistics camps near the border; the commitment of so-called "volunteer" combined-arms battalion's tactical groups; and the integration of proxy forces into higher-level formations that were commanded, supported, and equipped by the Russians (Phillip, 2015).

iv **Coercive Deterrence**: Secret strategic force alerts and snap checks include the aggressive air monitoring of nearby areas to prevent their involvement, the forward deployment of tactical nuclear delivery systems, theatre and intercontinental "in your face" manoeuvres, and more (Phillip, 2015).

v **Negotiated Manipulation**: The abuse and exploitation of ceasefires negotiated by the West to rearmament their proxies; the use of violations to deplete the enemy's Army while discouraging other states from lending support out of concern for escalation; the division of the Western alliance through the use of economic incentives and selective, repetitive phone talks that sway a preferred security partner (Phillip, 2015).

Russia's New-Generation Warfare in Ukraine: Implications for Défense Policy

After the disintegration of the USSR, the Soviet Union suffered greatly in terms of political, economic, and military affairs, and its global reputation was greatly affected. Henry Kissinger states, "Russia never considers Ukraine a foreign country". Ukraine has been regarded as a guarantor of Russia's territorial integrity and Belarus (Berzins, 2014). Previously, Russia has used modern defence strategies. Russia has extended its borders as part of the Soviet Union's expansion strategy. Russia was not willing to accept Baltic States joining NATO in 2004. As discussed, former Soviet countries will act as a neutral buffer zone (Bērziņš, 2014). Russia considers Ukraine a neutral country and a close friend. The interference of the US and EU in Ukraine is a direct threat to Russia's regional security interests. Russia would like to maintain good relations with Ukraine. Russia signed an agreement with Ukraine on February 21, 2014, to end protests facilitated and mediated by France, Poland, and Germany. Russia has vehemently condemned the funding of the West to Ukraine (Berzins, 2014).

The West has tried to destabilize the Yanukovych government through international non-government agencies. As part of the agreement, Russia directed Ukraine to continue the original form of the Ukrainian Constitution and establish a new central election commission. Russia would like to control the political elite of Ukraine through various diplomatic means to safeguard the security interests of Russia. President Yanukovitch has been impeached in the parliament of Ukraine (Bērziņš, 2014). President Yanukovitch and officials left the nation. All these developments led to the annexation of Crimea. Russia has stated that the impeachment of Yanukovitch was unlawful and that the new administration lacked political legitimacy. Impeachment can only be carried out when there is a three-fourths majority in parliament. The impeachment procedure was implemented in the Ukrainian Parliament without following the constitutional procedure. The officials in the new government have become a significant threat to the security and national interests of Russia as well as Ukraine. Russia has to protect the fundamental rights of Russian minorities. (Bērziņš, 2014). Ukraine has always been a red line for Russia.

Table 13.1 Russia's Arms Exports to Global Countries in the Contemporary World Order

Year	*Military Expenditure Database (in US$ millions)*	*Share of Government Spending(%)*
2010	58,720.2	10.12
2011	70,237.5	10.32
2012	81,469.4	10.84
2013	88,352.9	11.12
2014	84,696.5	11.77
2015	66,421.8	13.81
2016	69,245.3	14.83
2017	66,913.0	12.20
2018	61,609.2	11.40
2019	65,201.3	11.40
2020	61,712.5	10.59
2021	65,907.7	10.31
2022	102,366.6	12.94
2023	109,454.4	16.14

Source: Information from the Stockholm International Peace Research Institute (SIPRI) Military Expenditure Database, website: https://www.sipri.org/databases/milex

Russia has to protect its military and regional interests. The Russian Black Sea fleet has called Crimea home. Russia has established its military base in the Black Sea. Russia has played the role of an autonomous player, unlike the USA.

Russia deserves respect in Ukraine on par with the USA. Russia wants to protect its military, national and regional interests (Bērziņš, 2014).

Table 13.1 shows that Russia supplied arms to global countries worth TIV US$58,720.2 million in 2010. Russia exported arms worth TIV US$81,469.4 million in 2012; similarly, Russia supplied TIV US$84,696.5 million in 2014. Further, Russia supplied weapons worth TIV US$69,245.3 million in 2016. In 2018, Russia exported arms worth TIV US 61,609.2 million, which increased to US $61,712.5 million in 2020. Finally, Russia supplied weapons worth TIV US$102,366.6 million in 2022, which increased to US$109,454.4 million in 2023 (Stockholm International Peace Research Institute (SIPRI), 2023)

Russia's Campaign in Ukraine as New-Generation Warfare

Russia's military strategy has been divided into three phases: (i) Unilateralism doctrine states that force has to be effectively used to gain legitimacy; (ii) Defending Legalism: The legal institutions have approved all Russian activities. The Russian Parliament has approved the use of force in Ukraine as per the direction of Vladimir Putin. In the case of Crimea, Russia did not use force to maintain peace. (iii. Thirdly, Russia has contested that it did not use military troops to occupy while annexing Crimea. However, Indigenous self-defence forces stayed within the parameters of the diplomatic agreement

between Russia and Ukraine (Berzins, 2014). Pro-Russian political factions in Crimea have suggested the referendum, and Russia has supported the same idea. Russia strongly believes in the notion of self-determination, like the Kosovo model. The West has a different perspective on this narrative. The West has argued that it is against the Ukrainian Constitution, and that the ballot document did not mention whether or not Crimea would stay a part of Ukraine. Russia sees this analysis in terms of its own interests. Russia has stated that the result will be based on the outcome of its actions and policies towards Ukraine according to the international agreement signed in the 1990s (Berzins, 2014).

Similar scenarios were present in the 2008 operations in South Ossetia and Abkhazia. A strategic communication method has been employed in Crimea. By the end of 2020, Russia had used new military techniques and strategies. Some 190 of the military bases of Ukraine have been surrendered to Russia within three weeks, and their morale has been decimated without firing a single shot. This shows Russia's efficient use of new warfare methods. Russia has not deployed artillery and tanks in Crimea (Berzins, 2014). The Spetsnaz commandos and battalions of airborne troops have encountered Ukrainian forces. Wheeled BTR-80 armoured vehicle was also used in fighting the Ukrainian forces. After attacking the Ukrainian troops from their positions, Russia used the NGW techniques, i.e., intimidation, media, internet propaganda, psychological warfare, and bribery. Russia has defeated the opposition forces without using their forces.

Apart from new techniques, the display of contemporary people gears, light-wheeled armoured vehicles, Russian troops' exceptional discipline, and body armour have been used in the Russian army to showcase the strength of Russian troops (Berzins, 2014). Hence, Trends of Military Expenditure Share of Government Spending

Russia's share of government spending in 2010 was 10.12%, and it rose to 10.84% of the government's expenditure by 2012. Similarly, Russia's share of government spending was 11.77% in 2014 and increased to 14.83% in 2016. Russia's share of government spending was reduced to 11.40% in 2018 and 10.59% in 2020. Finally, the share of government spending increased to 12.94% in 2022, and the share of the government spending was 16.14% in 2023.

Table 13.2 shows that the United States is the major global arms exporter, supplying weapons worth TIV US$108,235 million from 2014 to 2023. Russia has emerged as the second largest arms supplier, with TIV US $45,867 million from 2014 to 2023. France stood in third place by exporting the defence equipment TIV US$25,657 million. Similarly, Germany has emerged as the fourth-largest arms supplier with TIV US$16,877 million. These countries were followed by China (TIV US$16,686 million), The United Kingdom (TIV US$11,093 million), Italy (TIV US$9235 million), Israel (TIV US$7974 million), Spain (TIV US$7766 million), and South Korea (TIV US$5290 million). The rest of the world exported weapons to the value of TIV US$30,038 million over the same period (Stockholm International Peace Research Institute (SIPRI), 2023).

Table 13.2 The Volume of Exports of Major Arms by the Top 10 Largest Suppliers 2014–2023 (US$ millions)

Rank 2014–2023	*Supplier*	*2014*	*2015*	*2016*	*2017*	*2018*	*2019*	*2020*	*2021*	*2022*	*2023*	*2014–2023*	*Share of Global Arms Imports(%)*
1	United States	9490	9868	9465	114,44	9576	10,908	9532	11,074	15,592	11,287	108,235	38
2	Russia	5335	5788	6706	6376	6901	5051	3523	2315	2603	1269	45,867	16
3	France	1768	2271	2141	2315	1879	3724	2387	3892	3268	2012	25,657	9.00
4	Germany	1822	1812	2509	1841	1110	997	1161	857	1481	3287	16,877	5.90
5	China	1327	1814	2445	1625	1358	1593	700	1310	2083	2432	16,686	5.90
6	United Kingdom	1658	1183	1324	1107	680	919	637	717	1665	1204	11,093	3.90
7	Italy	674	687	621	705	537	383	825	1650	1716	1437	9235	3.20
8	Israel	400	570	1236	1193	1147	384	395	619	870	1159	7974	2.80
9	Spain	962	982	481	820	705	308	981	619	970	940	7766	2.70
10	South Korea	220	94	437	702	1049	682	772	510	204	621	5290	1.90
	Others	3368	3284	3418	3073	2440	2269	2846	2790	3093	3458	30,038	11
	Total	27,023	28,353	30,784	31,200	27,380	27,219	23,758	26,352	33,544	29,104	284,718	100

Source: Information from the Stockholm International Peace Research Institute (SIPRI) Military Expenditure Database, website: https://www.sipri.org/databases/milex

Share of Global Arms Import

Table 13.2 stipulates that the share of the United States in global arms imports was 38% from 2014 to 2023. Russia's share was 16% of global arms imports. France has exported weapons with a percentage of 9.00%. The share of Germany's global arms import was 5.90%. China's share of global arms imports was 5.90%. The share of the United Kingdom was 3.90% from 2014 to 2023. The share of global arms imports in Italy was 3.20%. The share of global arms imports in Israel was 2.80%. The global arms import share of Spain was 2.70%. South Korea has contributed to 1.90% of global arms imports.

Table 13.3 shows that Saudi Arabia has emerged as the largest arms supplier by importing defence equipment to the value of TIV US$27,922 million from 2014 to 2023. It was followed by India (TIV US$26,894 million), Egypt (TIV US$13,243 million), Qatar (TIV US$12,819 million), Australia (TIV US$11,839 million), China (TIV US$11,087 million), Pakistan (TIV US$10,278 million), Algeria (TIV US$ 8545 million), South Korea (TIV US$8339 million), and, in tenth place, the UAE, with a total of weapons imports of TIV US$8150 million (Stockholm International Peace Research Institute (SIPRI), 2023).

Share of Global Arms Imports

In percentage terms, Table 13.3 explains that Saudi Arabia ranked first in global arms imports, importing 9.80% of defence equipment, and India ranked second, with 9.40%. These were followed by Egypt (4.70%), Qatar (4.50%), Australia (4.20%), China (3.90%), Pakistan (3.90%), Algeria (3.00%), South Korea (2.90%), and the UAE (also 2.90%).

Table 13.4 explains that the African region exported TIV US$1130 million in defence equipment from 2010 to 2023. The American region supplied arms worth TIV US$136,890 million during 2010–2023. Asia and Oceania supplied military equipment worth US$30,441 million from 2010 to 2023. Similarly, the European region supplied weapons worth TIV US$179,778 million from 2010 to 2023, And the Middle East supplied military equipment worth TIV US$14,952 million.

Percentage of share in world arms exports region-wise: The African region contributed 0.30%. The share of the Americas in world arms export was 38%. Asia and Oceania have contributed 8.40%. Similarly, Europe, including Russia, has accounted for 49%. The Middle East has exported 4.10% of the total weapons. The data above stipulates that Europe has extensively exported weapons, and 49% of world exports are to global countries. After the European region, the American region occupied second place by exporting 38% of defence equipment. During 2014–2018 and 2019–2023, European states increased their import of defence equipment by 94%. Meanwhile, arms transfer of world countries has fallen by 3.3%. The Middle East, Asia, and Oceania have continued to have a larger scale of weapon import than Europe. The Middle East, Asia and Oceania account for nine of the ten largest arms importers between

Table 13.3 Ranking of Exporters/Importers the volume of Imports of Major Arms by the Top 10 Largest Recipients 2014–2023 (US$ million)

Rank 2014–2023	*Recipient*	*2014*	*2015*	*2016*	*2017*	*2018*	*2019*	*2020*	*2021*	*2022*	*2023*	*2014–2023*	*Share of global arms imports(%)*
1	Saudi Arabia	2711	3384	2974	3968	3170	3065	2399	1803	3132	1315	27,922	9.80
2	India	3201	2724	2553	2656	2006	3147	2637	3959	2582	1428	26,894	9.40
3	Egypt	430	1443	1641	2462	1630	1091	1360	1325	733	1130	13,243	4.70
4	Qatar	55	488	596	321	691	2438	963	2077	3384	1805	12,819	4.50
5	Australia	857	1470	1029	1664	1582	1184	1650	1215	827	362	11,839	4.20
6	China	1041	1252	1223	1550	2029	1341	779	686	717	471	11,087	3.90
7	Pakistan	860	771	831	873	890	737	685	1035	1466	2129	10,278	3.60
8	Algeria	716	896	2914	1136	1287	167	600	162	313	355	8545	3.00
9	South Korea	742	268	1038	962	1030	1605	1273	812	423	189	8339	2.90
10	UAE	738	1186	946	832	1128	862	574	530	452	902	8150	2.90
	Others	15,671	14,474	15,037	14,776	11,938	11,583	10,838	12,748	19,516	19,019	14,5600	51
	Total	27,023	28,353	30,784	31,200	27,380	27,219	23,758	26,352	33,544	29,104	284,718	100

Source: Information from the Stockholm International Peace Research Institute (SIPRI) Military Expenditure Database, website: https://www.sipri.org/databases/milex

Table 13.4 The Volume of Exports of Major Arms by the Top 10 Largest Suppliers 2014–2023

	2010	*2011*	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*	*2019*	*2020*	*2021*	*2022*	*2023*	*2010–2023*	*% of world's total*
Africa	197	50	97	104	59	65	82	96	81	82	74	58	54	31	1130	0.30
Americas	8414	8705	8790	7525	9133	9581	8897	10,622	9273	10,745	9632	11,002	14,571	10,001	13,6890	38
Asia and Oceania	2032	1843	1782	2487	1518	2031	3054	2385	2442	2114	1431	1889	2318	3114	30,441	8.48
Europe	12,161	16,254	13,989	14,773	13,736	13,316	14,808	14,405	12,374	11,897	9968	10,675	11,463	9957	179,778	49
Middle East	728	740	707	680	664	790	1566	1473	1505	790	729	1164	1454	1964	14,952	4.10
Unknown/not applicable	23		1	5	5	2	2	5		2	2	8	13	12	80	0
World total	23,554	27,593	25,368	25,574	25,115	25,785	28,409	28,986	25,675	25,629	21,835	24,795	29,872	25,079	363,269	100

Source: Information from the Stockholm International Peace Research Institute (SIPRI) Military Expenditure Database, website: https://www.sipri.org/databases/milex

2019 and 2023, including Qatar, India and Saudi Arabia. More than 30 governments have extensively contributed to the transfer of weapons, and Ukraine has become the fourth-largest arms importer. The United States accounted for the 17% increase in arms exports during 2014–2023. Russia's shipments have decreased by 53%. Arms exports from France have increased by 47%, and they crossed Russia, which has always stood second in arms exports.

Contemporary Issues of Russia's New Warfare Methods

Russia has faced the following issues while using new warfare methods: In the case of hybrid warfare, Russia has faced technical issues, particularly concerning cyber operations, and some irregular tactics have also been used. Russia has used traditional military operations in the case of Syria. Russia has been facing various issues concerning cyber warfare. The role of private military corporations (PMCs) has also posed a challenge to the Russian political system and security. Russia has to modernize its defence industry and arms to deal with the NATO security forces. Russia has to develop strategic partnerships with other countries to evade the economic sanctions imposed by the West and NATO.

Issues and Challenges of Russia's Arms Exports to Global Countries in the Contemporary World Order

According to the Stockholm International Peace Research Institute (SIPRI) database, Russia has been the largest arms exporter to global countries. In this process, Russia has been facing various challenges concerning geopolitical tensions. In the case of the Middle East, Iran and Syria are importing defence equipment from Russia. It will pose a significant challenge to the western countries. Further, India and Pakistan also have been importing arms from Russia. It will upset the military balance in South Asia. Russia's engagement with European countries and other Western countries has been affected by the sanctions imposed by the US and EU. These restrictions have also affected the Russian defence technologies in defence industries (Defence News, 2019). Ever since the start of the Russia–Ukraine war, Russia has been encountering global arms market competition from Western countries. Thus, Russia has to maintain the quality of the military hardware and the prices. Supplying sophisticated weapons will also lead to instability and regional conflicts worldwide. Russia has to invest more in research and development of the defence sector since the Western countries and NATO member countries are upgrading their defence capabilities and technology. Russia has to adopt strict measures to prevent attacks on cyber security. Since Russia heavily exports defence equipment and arms to global countries, it will have diplomatic and political ramifications. Exporting arms to a few countries will also affect bilateral relations in the contemporary global world. Economic dependence on exporting arms to other countries will affect Russia's economic condition. Hence, rapid

developments are taking place in the contemporary global world. Russia has to bring innovative changes in the new warfare methods, defence technology, supply of advanced and modernized defence equipment, and active engagement with the global world.

The Impact of Artificial Intelligence and Technology on the Dynamics of New-Generation Warfare Methods and Arms Exports in the Contemporary World Order

The emergence of artificial intelligence (AI) and advanced military technologies has altered the dynamics of battle and dynamic global arms exports. New Generation Warfare (NGW) technology has supplanted traditional warfare techniques. It has been combined with cyberwarfare techniques, disinformation operations, and AI-powered weaponry (Clarke, 2020). AI-enhanced military technologies have become key aspects of the global arms trade since States have heavily depended on AI systems to gain strategic advantages. AI military technologies have played a vital role in the global arms trade since states increasingly use AI-powered systems to gain more strategic advantages. Thus, Artificial intelligence (AI) and modernized technologies have a more significant impact on modern warfare. AI will significantly influence the military strategy, arms exports and military strategy.

Artificial Intelligence in New-Generation Warfare

New-generation warfare methods have asymmetric strategies, i.e., autonomous combat systems, AI-enabled surveillance, and cyber warfare (Kania, 2019). Artificial intelligence has been playing a significant role in the New Generation of Warfare by utilizing the precision, speed, and effectiveness of military operations while decreasing the dependence on human decision-making (Scharre, 2018). This technological shift has introduced various key changes in warfare strategies: (i) Autonomous Weapons Systems: Militaries and armed forces can use the advanced and latest technologies, such as robotic combat units, drones with AI-powered technology, automated defence systems, and robotic combat units, to conduct precision strikes with minimum human intervention. These weapons have increased operational efficiency and raised ethical concerns about accountability and the issues of unintended escalation (Horowitz, 2022a(ii) Cyber Warfare and AI-driven Threats: AI enhances offensive and defensive cyber capabilities. Countries have been deploying artificial intelligence to hack critical infrastructure, cyber espionage, and misinformation campaigns to counter enemy camps and armed forces.

Artificial intelligence has had a tremendous influence on global stability and national security (Brundage et al., 2018). (iii) AI in Military Decision-Making: Machine learning algorithms have been analysing data related to movements and battlefield tactics. AI is playing a more significant role in effective decision-making. Overdependence on automation will risk warfare technologies

(Geist, 2019). (iv) The Role of AI in Arms Exports and Geopolitical Influence: Artificial intelligence has been pivotal in the global arms trade and in influencing strategic alliances and global power politics. The top global arms exporters, Russia, the USA, and China, have effectively used the defence system with AI to maximize their geopolitical significance (Stockholm International Peace Research Institute [SIPRI], 2023a).

The impact of AI on arms exports includes: (i) Global Competition in AI-based Defence Technology: AI-driven technology has increased the arms race and modernized military systems. Countries have allocated funds and given importance to developing research in defence capabilities (Bitzinger, 2021). Russia, China, and the United States dominate the global arms market, leading to rivalries in defence technologies (Kleinhans, 2020). (ii) Proliferation of Autonomous Weapons: Since there has been an increase in the high level of usage of artificial intelligence, unmanned combat aerial vehicles have also increased. AI is strengthening military partnerships. Non-state actors also play a significant role in escalating conflicts (Gilli & Gilli, 2021(iii) Economic and Political Leverage Through Defense Exports—Challenges and Ethical Concerns: AI-powered weapons have been playing a vital role in influencing politics. Nations have used the transfer of military technology to develop strategic partnerships with global countries and their influence in the region. Ferguson (2022). Thus, it has played a vital role in the security landscape of Eastern Europe, the Middle East and Asia.

Various challenges have been associated with the use of AI in arms trade and warfare. The integration of AI has raised various legal, security, ethical, and critical questions. (i) Lack of International Regulations: There is an absence of international frameworks governing Artificial Intelligence. Autonomous weapons have been posing challenges, with special reference to international humanitarian law. Thus, rules and regulations must be formulated to govern AI-driven technologies in the contemporary world (Boulanin & Verbruggen, 2017). (ii) Risk of Escalation and Unintended Consequences: Warfare with Artificial Intelligence has increased the possibility of accidents due to the misinterpretations of automated systems (Payne, 2021). The decision-making power vested with AI will lead to various issues and raise concerns about the usage of advanced military weapons. (iii) Cybersecurity Threats and AI Weaponization: Cyberattacks using AI-driven technology and military infrastructure have grown rapidly. State and non-state actors have been exploring various options to gain strategic advantages (Taddeo, 2019). Disinformation campaigns using AI weaponization will also threaten social stability and democratic institutions.

Future Implications and Challenges of New-Generation Warfare Methods and Arms Exports in the Contemporary World Order

Developing New-Generation Warfare methods and the arms trade will challenge global strategic stability and security. The evolution of New Generation Warfare (NGW) technologies, autonomous systems, and cyber tools should

fall into the hands of non-state actors. There are no adequate international regulations to control cyber-attacks on AI-driven military technologies. Hence, it will lead to potential risks in the contemporary global world (Boulanin & Verbruggen, 2017). (i) The Changing Nature of Deterrence: Traditional military deterrence heavily depends on conventional military capabilities and nuclear facilities. The present military technologies are driven by AI-driven decision-making, lethal autonomous weapons and the rise of cyber warfare, and these have complicated military deterrence strategies. Countries must implement their defence policies to resolve various threats while preventing escalations. (ii) Ethical and Legal Considerations: Various ethical and legal issues have been associated with the New-Generation Warfare (NGW) methods. Autonomous weapons and the integration of AI have raised various legal and ethical questions about accountability in warfare. The global community and international organizations must formulate regulations to regulate cyber spyware and the misuse of AI-driven defence technologies (Garcia, 2019). NGW techniques are very important for the global security environment. Arms exports have served geopolitical interests. AI-driven technologies have led to instability in collaboration with the New-Generation Warfare methods. Effective regulatory mechanisms are required to control the AI-driven military technologies and cyber spyware. Global countries have to develop the regulatory frameworks to ensure global peace and harmony.

Future Implications and Policy Recommendations

Global policymakers must formulate guidelines for implementing measures to address various strategic issues and ensure stability in the global arms market. Key recommendations include: (i) Promoting Responsible AI in Military Applications: Defence organizations and governments must prioritize developing Artificial Intelligence (AI) to ensure autonomous decision-making and prevent the misuse of conflicts (Danks & London, 2017). (ii) Enhancing AI Security Measures: Countries must invest in cyber security frameworks to protect AI-driven military technology from adversarial attacks and cyber threats (Gady, 2022); (iii) Establishing International Regulations on AI in Warfare: The global community must develop mechanisms to regulate cyber warfare weapons to ensure accountability and ethics (Future of Life Institute, 2020).

Conclusion

The 21st century has brought out dynamic changes in the military warfare methods. Arms exports have been playing a vital role in the modern military technologies. New-Generation Warfare (NGW) techniques have also played a vital role in the global security. Modernized military technologies, artificial intelligence (AI), and autonomous weapons have all contributed to the complex scenario in the contemporary multipolar world order. Arms exports and imports have played a significant role in foreign policy strategies. Further, arms

exports influence global power structures and determine strategic alliances' future. Russia, the United States, and China have used advanced military technology transfers to strengthen their impact on geopolitics. The development of modernized and advanced weapons, i.e. hypersonic cruise missiles, cyber warfare tools and drones, have been facilitating the exacerbation of the armed conflicts, i.e. Sino-Russian military collaboration and AUKUS. Technological rivalries and high-level competition have determined global security.

NGW methods and arms exports have raised questions about strategic, ethical, and legal concerns. The lack of international regulations related to governing AI-driven military technology and cyber warfare tools has posed a serious threat to conflict escalation and the violation of sovereignty. Countries have been giving more importance to geopolitical interests than human rights considerations. Nations are promoting the privatization of military camps and the commercialization of defence technologies. Global mechanisms are required to address the issues associated with the New Generation of Warfare methods. Governments must develop mechanisms and norms for regulating cyber security spyware and disinformation camps. A framework must be developed to prevent the arms race in the contemporary world order. Foreign policymakers must play a significant role in balancing military deterrence and arms control initiatives. New-Generation Warfare methods and arms exports have been reshaping global security. States have to adopt new security initiatives to ensure international stability. Nations have to allocate funds for research and development related to the impact of technology on warfare, hybrid threats, the impact of private actors on the defence industry and strategies related to controlling arms proliferation. International organizations and nations must develop regulatory frameworks to end regional tensions and ensure security, peace and stability in the contemporary world order. In contemporary times, Russia has significantly devised its innovative military policy and arms export regulations, significantly impacting the global military environment. Russia has adopted NGW methods, such as hybrid warfare, information warfare, cyberwarfare, and private military contractors (PMCs).

Advanced Weaponry and Modernization: Russia has been increasingly using hybrid warfare, which combines traditional military force and political manipulation with economic pressure, cyber warfare, information operations, and political manipulation. It has been used immensely and at a high level in armed confrontations. Russia's contemporary strategy has been revolving around cyber activities and information warfare. It will lead to interference in the decision-making process and affect democratic institutions. The best examples were meddling in the US presidential election in 2016 and cyber-attacks on European countries. With the help of Private Military Contractors (PMCs), such as the Wagner Group, Russia has engaged military contractors in crisis areas like several African nations, Ukraine, and Syria. Russia has succeeded in these crises without using force. Russia has used modernized weapon systems. It has been heavily investing in the defence industry to modernize the armed

forces, develop innovative technology, and develop hypersonic missiles, modernized warfare systems, and advanced drone technology. Russia's modernized defence capabilities will strengthen NATO capabilities.

Russia has been developing strategic alliances with Africa, the Middle East and Asia and increased its influence at the global level. India, China, Algeria, and Egypt have heavily imported defence equipment from Russia. The image of Russia has increased in the contemporary multipolar world order. The Russian defence industry has been using innovative technology and exporting weapons to developing countries. Russia has been extending its cooperation regarding technology transfer to its strategic allies. Since the West has created arms competition in the global arms market, Russia has been modernizing its defence equipment and supplying qualitative defence equipment to its strategic allies. In the case of India, Russia has military-technical-economic cooperation and joint ventures in the defence sector, with particular reference to the joint development of weapons and technologies. Russia has firmly dealt with the economic sanctions imposed by the West.

Russia is playing a pivotal role in the contemporary world order. Russia has been developing strategic partnerships with India, China and North Korea. Russia has modernized its defence technology and new warfare methods to challenge the hegemony of the West. Thus, Russia prioritizes advanced defence technology and develops good relations with strategic alliances. Russia is playing a significant role in the contemporary multipolar world order in order to increase its significance in various multilateral forums, i.e. Brazil, Russia, India, China, South Africa (BRICS), Russia–India–China Trilateral Summit (the RIC Summit), the Shanghai Cooperation Organization (SCO), EURASIA and the Eurasian Economic Council (EEC). Russia is exporting qualitative defence equipment to countries in Asia and Africa. Thus, Russia has vehemently condemned the liberal internal order dominated by the West in the contemporary multipolar world order.

Bibliography

Bapat, N. A. (2012). Understanding state sponsorship of militant groups. *British Journal of Political Science*, *42*(1), 1–29.

Berzins, J. (2014). *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. National Defence Academy of Latvia, Center for Security and Strategic Research. https://www.naa.mil.lv/en/research/publications

Bērziņš, J. (2014). Russia's new generation warfare in Ukraine: Implications for defense policy. *Journal of Military Operations*, *2*(4), 05. Retrieved April 17, 2024, from https://www.tjomo.com/article/russias-new-generation-warfare-in-ukraine-implications-for-defense-policy/

Bērziņš, J. (2020). The theory and practice of new generation warfare: The case of Ukraine and Syria. *The Journal of Slavic Military Studies*, *33*(3), 355–380. Retrieved April 19, 2024, from https://doi.org/10.1080/13518046.2020.1824109

Bitzinger, R. A. (2021). *The emerging global arms race in artificial intelligence and autonomous weapons*. Routledge.

Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Stockholm International Peace Research Institute (SIPRI).

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Clarke, R. A. (2020). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Danks, D., & London, A. J. (2017). Regulating autonomous systems: Beyond standards. *IEEE Intelligent Systems*, *32*(1), 88–91.

Defense News. (2019, October 15). *Sanctions hit Russia's defense industry hard, limiting access to technology and markets*. https://www.defensenews.com/

Defence News. (2019, May 27). *Sanctions on Russia having ripple effects on global arms industry*.https://www.defensenews.com/global/europe/2019/05/27/sanctions-on-russia-having-ripple-effects-on-global-arms-industry/

Fabian, S. (2019). The Russian hybrid warfare strategy is neither Russian nor strategic. *Defense & Security Analysis*, *35*(3), 308–325. Retrieved May 17, 2024, from https://doi.org/10.1080/14751798.2019.1640424

Feldstein, S. (2020). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Ferguson, C. (2022). AI, geopolitics, and the future of arms exports. *International Affairs Review*, *98*(2), 45–60.

Future of Life Institute. (2020). *AI and autonomous weapons: Risks and regulation*. Retrieved from https://futureoflife.org

Gady, F. S. (2022). Cybersecurity and AI-driven warfare: Challenges and opportunities. *Journal of Strategic Studies*, *45*(3), 1–25.

Galeotti, M. (2016a). Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies*, *27*(2), 282–301. Retrieved April 15, 2024, from https://doi.org/10.1080/09592318.2015.1129170

Galeotti, M. (2016b). Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies*, *27*(2), 282–301. Retrieved May 15, 2024, from https://doi.org/10.1080/09592318.2015.1129170

Galeotti, M. (2019a). *Russian political war: Moving beyond the hybrid*. Routledge.

Galeotti, M. (2019b). *Russian political war: Moving beyond the hybrid* (1st ed.). Routledge. Retrieved April 02, 2024, from https://doi.org/10.4324/9780429443442

Garcia, D. (2019). *Disarmament diplomacy and human security: Regimes, norms and moral progress in international relations*. Routledge.

Geist, E. (2019). It's already too late to stop the AI arms race—We must manage it instead. *Bulletin of the Atomic Scientists*, *75*(1), 25–31.

Gilli, A., & Gilli, M. (2021). Military robotics and the proliferation of AI weapons. *Security Studies*, *30*(2), 189–215.

Horowitz, M. C. (2019). Artificial intelligence and international security. *International Security*, *44*(3), 7–36.

Horowitz, M. C. (2022a). *Artificial intelligence and the future of war*. MIT Press.

Horowitz, M. C. (2022b). The promise and peril of military AI. *Foreign Affairs*, *101*(3), 20–31.

Kania, E. (2019). China's military-civil fusion strategy and the implications for global security. *Journal of Defense Studies*, *35*(1), 45–61.

Karber, P. A. (2015). *Russia's new generation warfare*. National Geo-Spatial Intelligence Agency. Retrieved May 02, 2024, from [URL].

Karp, A. (2022). Turkey's ascent in the global defense market. *International Security Review*, *47*(3), 56–78.

Kim, H. (2023). South Korea's defense exports: Opportunities and challenges. *Journal of Defense Economics*, *15*(2), 112–134.

Kırdemir, B. (2022). Drone warfare and its implications for modern conflicts. *Defense Studies*, *22*(1), 45–67.

Kleinhans, J. P. (2020). *The geopolitics of AI-driven arms trade*. European Council on Foreign Relations.

Kundu, N. (2020). China–Myanmar military cooperation: Strategic imperatives and risks. *East Asia Forum*, *12*(2), 89–101.
Marsh, N. (2021). *Small arms, crime, and conflict: Global trends and challenges*. Oxford University Press.
Muradov, I. (2022). The Russian hybrid warfare: The cases of Ukraine and Georgia. *Defence Studies*, *22*(2), 168–191. Retrieved April 05, 2024, from https://doi.org/10.1080/14702436.2022.2030714
Nakashima, E. (2018). *Russian hackers' attack on critical infrastructure*. The Washington Post.
Payne, K. (2021). Artificial intelligence and deterrence: Assessing the risks. *Survival*, *63*(2), 45–70.
Phillip, A. (2015). *Understanding hybrid warfare: Political subversion and the undermining of democratic institutions*. Strategic Studies Institute, US Army War College.
Ripley, T., & Jones, S. (2014). Russia's hybrid warfare strategy and the Ukraine crisis. *Jane's Intelligence Review*, *26*(6), 8–13.
Schneider, J. (2020). *Artificial intelligence and future warfare: Implications for military strategy and policy*. Oxford University Press.
Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
SIPRI. (2023). *Trends in international arms transfers 2023*. Stockholm International Peace Research Institute.
Small, A. (2022). *The China–Pakistan axis: Asia's new geopolitics*. Oxford University Press.
Smith, M. A. (2019). *Russia and NATO since 2000: From Cold War through cold peace to partnership?* Routledge.
Stockholm International Peace Research Institute (SIPRI). (2023a). Trends in international arms transfers. SIPRI Fact Sheet. Retrieved from https://www.sipri.org/publications
Stockholm International Peace Research Institute (SIPRI). (2023b). Trends in international arms transfers. *SIPRI Yearbook*.
Stockholm International Peace Research Institute. (2024a). *The volume of exports of major arms by the top 10 largest suppliers 2014–2023*. Retrieved April 10, 2024, from https://www.sipri.org/databases/regional-coverage
Stockholm International Peace Research Institute. (2024b). *The volume of major arms exports by the top 10 largest suppliers 2014–2023*. Retrieved April 10, 2024, from https://armstransfers.sipri.org/ArmsTransfer/ImportExportTop
Stockholm International Peace Research Institute. (2024c). *The volume of major arms imports by the top 10 largest recipients 2014–2023*. Retrieved April 05, 2024, from https://armstransfers.sipri.org/ArmsTransfer/ImportExportTop
Taddeo, M. (2019). AI in cyber conflict: The automation of cyber attacks and the future of cybersecurity. *Philosophy & Technology*, *32*(3), 369–372.
Wezeman, P. D., et al. (2023a). *Trends in international arms transfers, 2022*. SIPRI.
Wezeman, P. D., Fleurant, A., Kuimova, A., Tian, N., & Wezeman, S. T. (2023b). *The impact of Russia's war on global arms transfers*. SIPRI Policy Brief.
Wezeman, P. D. (2024). *Trends in international arms transfers 2023*. SIPRI Fact Sheet 2024. Retrieved April 05, 2024, from https://www.sipri.org/sites/default/files/2024-03/fs_2403_at_2023.pdf
Winter, C. (2018). *The ISIS propaganda machine: A case study in terrorism and technology*. Hurst Publishers

14 Understanding the Impact of Emerging Technologies on Wars

Ramifications for India

Devesh Vatsa

Introduction

In the classic sense, war meant several military campaigns in which at least two parties consisting of large masses of people and fighting equipment were in opposition to issues of sovereignty, territory, resources and power and clashed directly to impose will or a certain behaviour by force(Cristian, 2015). Warfare, which is as old as human civilization, has always been at the forefront of civilization. The race on the battlefield has been with the intention of achieving competitive advantage over the enemy, which led warriors to don the inventor's hat and bring about a lot of developments which eventually created the timeline of the evolution of warfare (Sengupta, 2021). Over the centuries, warfare has progressed from primitive wars between tribal societies to conflict between societies based on the agrarian economy and further, to eventually to armed conflicts between industrialized societies. Mankind has progressed successively from fighting with bows and arrows to the deployment of rifles, guns, tanks, aircraft and missiles (Anand, 1999). The evolution of warfare has been driven by the development of new technologies and the changing nature of societies. Early warfare began with tribal societies fighting with primitive weapons such as sharpened stones. Chariots were a major development in the early 400s BCE, giving the user an advantage of speed and agility. The decline of chariot warfare as a dominant force in battles was a gradual process, influenced by factors like the development of more effective infantry tactics, including those of the Roman legion, and improvements in cavalry. The cavalry knight, or "mounted terror", was a significant development that emerged from the desire to combine the chariot's competitive advantage with the deployment of armed legions. Similarly, the introduction of gunpowder was a key development in the evolution of warfare. Modern conflict has seen the development of weapons of mass destruction, including rifles, guns, tanks, aircraft, and missiles. Second Generation Warfare (2ndGW) was characterized by trench warfare and linear fire and movement warfare. Some cultural evolutionary theories argue that military technologies have resulted in "Military Revolutions" which that have had major ramifications for the rise of state formations (Figure 14.1).

DOI: 10.4324/9781003633204-17

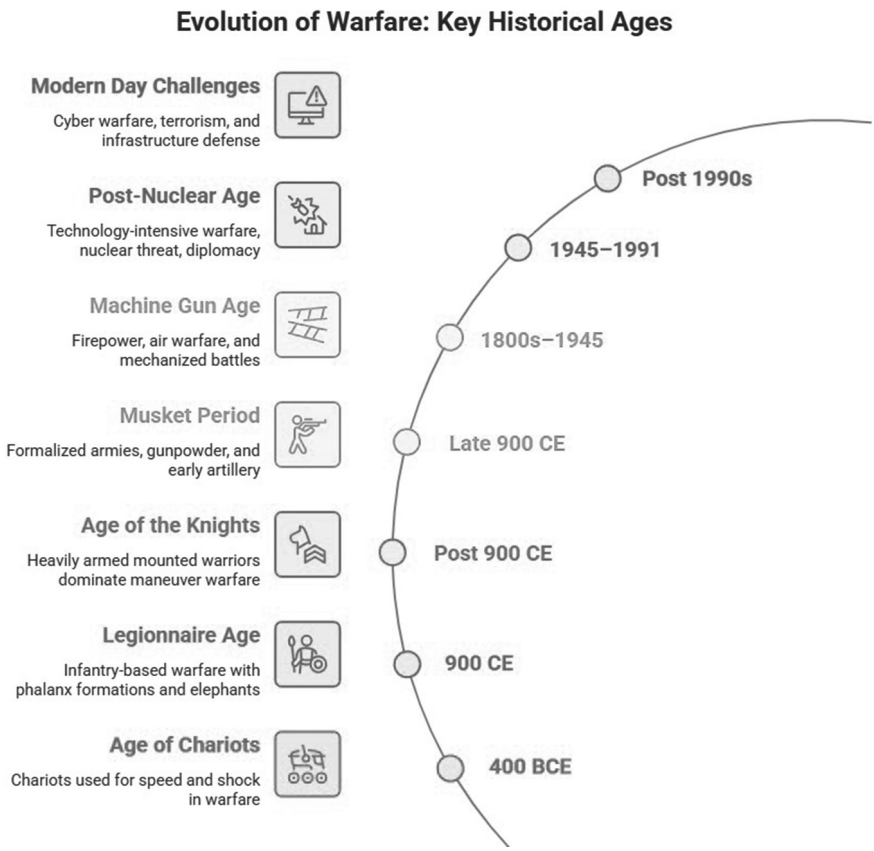

Figure 14.1 Evolution of Warfare.

Technology, from a warfighting perspective, has undergone significant evolution over the centuries, which has "impacted warfare in a profound manner, according to Army Chief General Manoj Pandey (Press Trust of India, 2024). He underlined how history shows that those armies that have managed to adopt and integrate new technologies have secured an advantage on the battlefield and achieved success. The rapid evolution of emerging technologies is reshaping the landscape of warfare, fundamentally altering how conflicts are fought and won. Emerging technologies have increased the lethality and accuracy of weapons and have also changed the way wars are fought. These technologies have also created new types of warfare, such as cyber warfare and space wars. In this context, India stands at a critical juncture, facing unique challenges and opportunities as it seeks to enhance its military capabilities in response to regional threats, particularly from China and Pakistan. This chapter delves into the implications of disruptive technologies such as artificial intelligence, autonomous systems, cyber warfare, and quantum computing for

India's defence strategy. As nations around the world invest heavily in these technologies, the Indian military must adapt to maintain its strategic edge. The integration of advanced systems not only enhances operational effectiveness but also redefines traditional concepts of deterrence and warfare. However, technology alone does not guarantee success; it must be effectively incorporated into military strategy and tactics. This chapter will explore how India is navigating these complexities, focusing on the development of indigenous capabilities and the ethical considerations surrounding new paradigms of warfare. By examining the interplay between emerging technologies and military operations, this chapter aims to provide a comprehensive understanding of how India can leverage these advancements to bolster its defence posture while simultaneously addressing the multifaceted challenges posed by an increasingly competitive geopolitical landscape.

Emerging Technology

These are technologies whose development or practical applications (or both) are still largely unrealized. These technologies are generally new but also include old technologies which are now finding new applications. Emerging technologies are often perceived as being capable of changing the status quo. This is a term generally used to describe new technology, but it may also refer to the continuing development of an already existing technology; it can have slightly different meanings when used in different areas, such as media, business, science, or education. The term 'emerging technology' commonly refers to technologies that are currently developing, or that are expected to be available within the next five to ten years. It is usually applied to technologies that are creating, or are expected to create, significant social, military or economic effects. They have the potential to reshape industries, economies and societal structures, presenting both opportunities and challenges for organizations of all sizes and types (Report World Economic Forum, 2024).

> History informs us that those who are first to harness once-in-a-generation technologies often have a decisive advantage on the battlefield for years to come.
>
> Former US Defense Secretary Dr Mark Esper

Emerging Technologies in Warfare

Military conflict in the coming decades will also be driven by the similar factors that have historically prompted wars. However, the ways in which war is waged will change with adoption of new technologies and the induction of modern weapon systems enabled by AI, new applications, and emerging doctrines factoring that additional actors also gain access to these capabilities. The reasons behind any conflict range from resource protection, border integrity, economic disparities, and ideological differences to the pursuit of power and influence.

The combination of improved sensors, automation, and artificial intelligence (AI) with hyper-sonics and other advanced technologies will produce more accurate, better-connected, faster, longer-range, and more destructive weapons. These will be primarily available to the most advanced militaries, although some will be within reach of smaller state and non-state actors (An Introduction to the Building Blocks of Global Trends, 2021). Over time, the proliferation and diffusion of these systems will make more assets vulnerable, heighten the risk of escalation, and make combat potentially more deadly, though not necessarily more decisive. Modern warfare has continuously evolved, with technological advancements generally shaping these developments. Technological advances have given rise to new methods and mean of warfare, such as cyber-attacks, armed drones and robots.

Critical technologies like cyberspace and AI are making new warfighting tools available, even as traditional ones such as nuclear weapons are witnessing a resurgence. These changes have brought greater lethality and destruction in warfighting and blurred the lines of conflict, with direct warfare being replaced by new forms such as hybrid warfare or grey zone tactics (where the threat has diffused, and proxy actors have taken the lead) (Rajagopalan & Patil, 2024). Emerging technologies have a significant impact on war, increasing the speed, accuracy and lethality of weapons, and enabling new forms of warfare. Increased speed, accuracy and lethality are achieved through: *Advanced surveillance technologies*, which can locate enemy forces, allowing for more accurate targeting; *Satellite-provided imagery*, which can improve the accuracy of weapons systems; and *Hypersonic systems*, which can strike targets at great distances with unprecedented speed and maneuverability. The militaries of top countries are keeping pace by adapting and adopting innovations to gain strategic advantages. From strengthening cyber defences to integrating artificial intelligence, future military technology promises to bring significant changes (Figure 14.2).

Let us examine some few of the future military technologies that are set to transform defence strategies and impact the way in which future wars will be fought. Future wars will be network-centric and will be enabled by multiple technologies, as shown in Figure 14.3.

Unmanned Systems and Drones: Unmanned systems, including drones and autonomous vehicles, are becoming indispensable in modern military operations. These technologies serve multiple roles, including intelligence, surveillance, reconnaissance (ISR), logistics support and combat operations. Unmanned Aerial Vehicles (UAVs) gather intelligence, carry out precision strikes, and monitor enemy movements. By contrast, unmanned ground vehicles (UGVs) can handle dangerous tasks such as bomb disposal and supply delivery. By taking on hazardous and repetitive tasks, autonomous systems will increase operational flexibility and reduce the risk to human soldiers (Singh, 2024) The ability to deploy drones equipped with advanced sensors and AI allows for real-time data analysis and quicker decision-making, significantly enhancing operational effectiveness. For instance, during recent conflicts such as the Armenia–Azerbaijan war and the Russia–Ukraine conflict, drones have demonstrated their value in

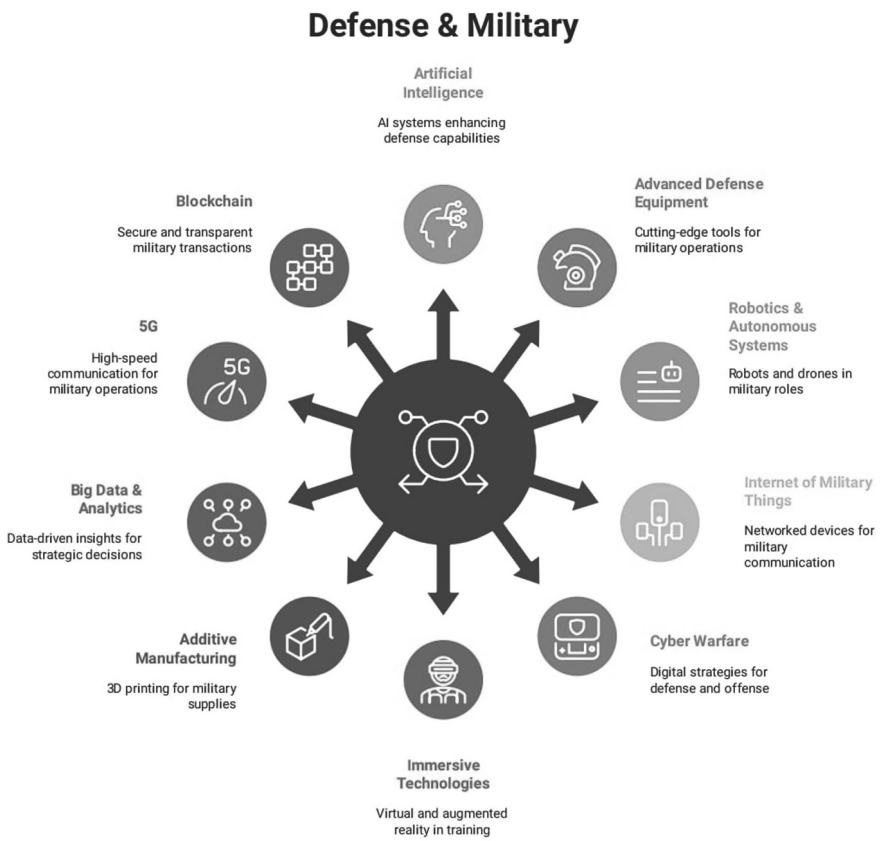

Figure 14.2 Top future military technologies.

both offensive and defensive operations (Bommakanti et al., 2024). Drones are growing in importance for several reasons, including: *Real-time logistics*: Drones can provide live video feeds anywhere on the battlefield without the need for satellite imagery; *Targeting*: Unlike artillery, drones can target specific areas, vehicles and soldiers; *Suppression*: Drones can be used to suppress missile and air attacks. However, the main reason behind the increasing use of drones may be *economics*. Drones are exceedingly cheap to produce when compared to most other weapons. Cheap drones can easily destroy many expensive, high-tech weapons on the battlefield, resulting in a large economic advantage for the side deploying them. For example, drones used by Houthi rebels cost around $2,000 each. However, it costs the US military $2M to shoot just one down (Seligam & Berg, 2020). Similarly, Ukraine now has a dedicated "commander of drone forces" (Reuters, 2024). These stories clearly indicate the increased and significant role of drones in the future battlefield.

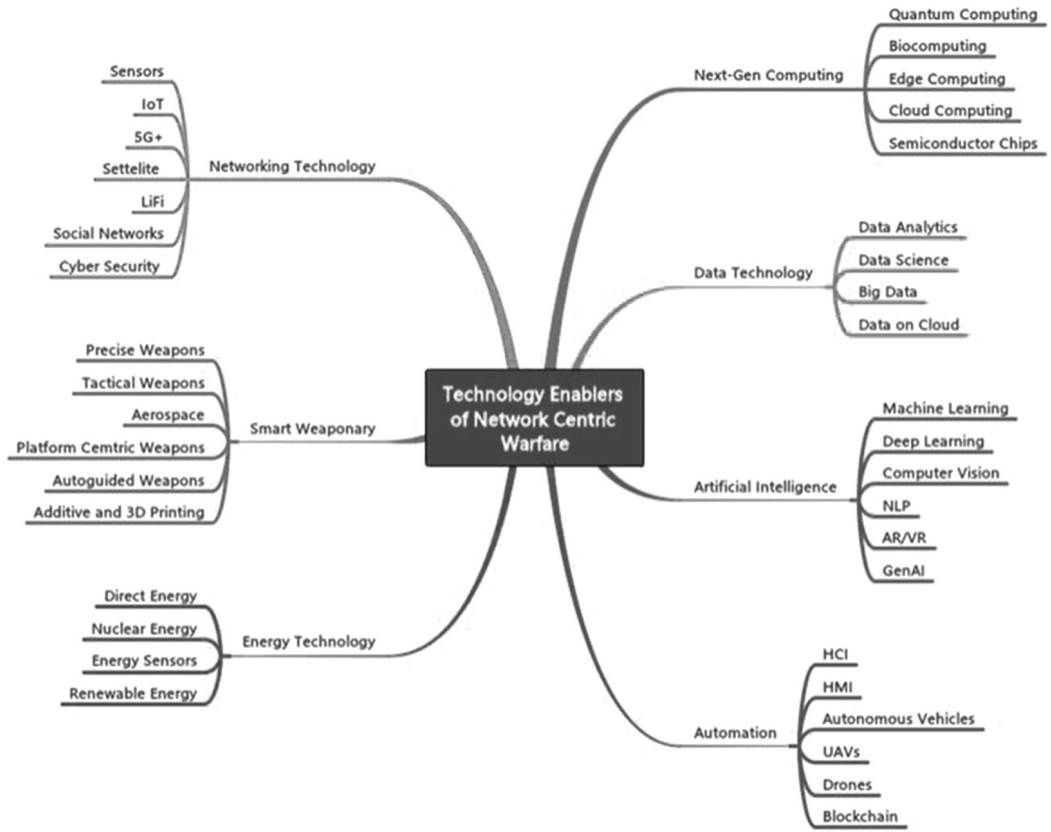

Figure 14.3 Technology enablers of network-centric warfare.

Artificial Intelligence (AI)

Artificial intelligence (AI) is a transformative technology which can revolutionize defence strategies by offering diverse capabilities to enhance operational efficiency and decision-making processes. AI applications in defence span various domains, including air traffic management, fuel consumption optimization, and intelligence and surveillance operations. By leveraging AI algorithms, defence systems can optimize airspace utilization, reduce fuel costs, and process vast amounts of data to derive actionable insights for informed decision-making. For example, AI-driven solutions in air traffic management enable real-time airspace monitoring, route optimization, and collision avoidance, thereby enhancing aviation safety and efficiency. Furthermore, one of the most significant impacts of AI in defence is the development of autonomous weapons systems. These AI-powered systems are designed to operate independently, making precise and accurate split-second decisions in combat scenarios. By integrating AI into defence applications, autonomous weapons systems can enhance military capabilities, improve response times, and potentially reduce human intervention in high-risk situations. For instance, the deployment of autonomous drones equipped with AI algorithms enables rapid surveillance, target identification, and strike operations, showcasing the evolving landscape of defence technologies toward more autonomous and intelligent systems. AI is making decision-making smarter, making operations more efficient, and threat predictions more accurate. AI can sift through massive amounts of data to spot patterns, predict potential threats, and assist in strategic planning. On the battlefield, AI algorithms can control autonomous vehicles, manage supply chains, and even carry out precision strikes with minimal human involvement. Having AI in military systems will speed up and sharpen responses in combat situations.

AI is revolutionizing military strategy by improving decision-making processes and operational efficiency. The Indian military is increasingly leveraging AI to enhance its ISR capabilities, optimize logistics, and improve firepower accuracy. AI-driven systems can analyse vast amounts of data rapidly, allowing commanders to make informed decisions in real time. This capability is crucial for India's military strategy as it seeks to counter threats from technologically advanced adversaries (Sharma, 2023)

Cyber Warfare

Cyberwarfare has rapidly advanced from a niche area to becoming a core element of national security. Given the increased dependency of today's military operations on digital networks, this automatically makes them a soft target for sophisticated cyber-attacks. Advanced persistent threats (APTs) and ransomware can disrupt command-and-control systems and cripple logistics, making it easy to steal sensitive data. In the future, cyber warfare will see even more advanced offensive and defensive tactics, including the use of AI-driven

cybersecurity systems (Oledcomm, 2024). These systems can detect and neutralize threats almost instantaneously. Cyber capabilities are becoming integral to national defence strategies. The ability to conduct cyber operations can disrupt enemy communications, gather intelligence, and protect critical infrastructure. India faces significant cyber threats from both state and non-state actors, necessitating a robust cyber defence strategy that includes offensive capabilities to deter potential aggressors (Junaid, 2024)

Space Warfare

The militarization of space is another critical area in which emerging technologies are influencing warfare. Countries are increasingly developing capabilities to operate in space for reconnaissance, communication, and navigation purposes. The domain of space has become increasingly critical for national security, with the establishment of the Defence Space Agency (DSA) underscoring the strategic importance of space operations in defence strategies. Advanced satellite technology, driven by the growing demand for geospatial intelligence and imagery, has transformed space into a critical domain for the enhancement of defence capabilities. For instance, satellite communication systems enable secure and reliable data transmission for military operations, facilitating real-time situational awareness and communication in remote and hostile environments. By leveraging satellite technology, defence organizations can enhance surveillance, reconnaissance, and communication capabilities, enabling effective command and control of military assets across diverse operational theatres.

Moreover, integrating satellite surveillance capabilities has revolutionized defence strategies by providing persistent monitoring and intelligence-gathering capabilities. Defence entities can track and analyse global activities, detect potential threats, and respond proactively to emerging security challenges by deploying satellite constellations equipped with high-resolution imaging sensors and advanced data analytics. For example, satellite reconnaissance missions enable defence forces to monitor adversary movements, assess infrastructure developments, and gather intelligence on potential threats, contributing to strategic decision-making and operational planning. The synergy between space operations and defence strategies highlights the industry's commitment to leveraging space as a force multiplier, extending the reach and capabilities of military forces for enhanced national security. India's advancements in satellite technology enhance its strategic position by providing vital information about adversary movements and capabilities (Dwivedi, 2023)

Hypersonic Missiles

The race for Hypersonic Technology has become a focal point in defence innovation, with countries investing heavily in developing superior hypersonic capabilities for military applications. Hypersonic weapons, capable of traveling at speeds exceeding Mach 5, offer significant advantages in speed, precision, and

evasive maneuverability, reshaping the dynamics of modern warfare. They are designed to evade traditional missile defence systems with incredible speed and maneuverability. Hypersonic missiles can deliver powerful payloads with pinpoint accuracy, making them a formidable tool in modern warfare. Directed Energy Weapons (DEWs), such as high-powered lasers and electromagnetic railguns, are among the advanced defence technologies being explored to enhance military capabilities and counter emerging threats. The pursuit of hypersonic technology aims to outpace adversaries, maintain strategic superiority, and ensure deterrence in an increasingly contested security environment. It is expected that future military technology will focus on improving guidance systems, increasing range, and developing effective countermeasures. For example, the United States, China, and Russia actively pursue the development of hypersonic weapons to gain a strategic edge and deter potential adversaries. Countries that have developed hypersonic missile technology include India, Russia, China, and the US. Other countries that have developed hypersonic weapons include Australia, Brazil, France, Germany, Iran, Japan, North Korea, South Korea, and United Kingdom.

Digital Healthcare Automation

Modern healthcare automation is transforming military medicine by making it easier to manage and use health data, which ultimately leads to improved care for service members. Automated systems simplify patient record-keeping, enable remote diagnostics, and ensure timely medications. Wearable health monitors and telemedicine platforms are also becoming increasingly common. They help track soldiers' health in real time, provide immediate medical support if required, and reduce the burden on field medics. These advancements keep the troops ready and lead to improved medical outcomes, both during peacetime and in combat situations.

Internet of Military Things (IoMT)

The Internet of Military Things (IoMT) involves the integration of various devices and sensors into a cohesive, intelligent military network. By using interconnected devices, ranging from wearable sensors to advanced surveillance systems, IoMT provides real-time communication and actionable insights. This interconnected ecosystem improves situational awareness and coordination and boosts operational efficiency. In future military operations, IoMT will offer a comprehensive view of the battlefield. This will, in turn, aid in better decision-making and ensure synchronized efforts across various military units.

LiFi for Communication

Light Fidelity (LiFi) feels like a future military communication technology, but it is already here. Instead of using traditional radio frequency for communication, LiFi uses light to transmit data. The system operates by modulating light

from LED sources to encode information and allows for high-speed data transfer with minimal interference. In military settings, LiFi is particularly valuable for its ability to provide secure, localized communication networks. This makes LiFi ideal for control and command centres and tactical operations where reliability and speed are crucial.

Virtual Reality (VR) & Augmented Reality

Virtual Reality (VR) and Augmented Reality (AR) technologies are transforming the way in which soldiers are trained, and missions are planned. VR offers immersive simulation environments for training exercises, allowing soldiers to practice and respond to various combat scenarios without real-world risks. In contrast, AR overlays digital information onto the physical environment and takes situational awareness to a whole new level by providing real-time data during missions. By creating interactive and data-rich environments, these technologies make training and operational planning more effective and efficient.

Military Robotics & Autonomous Systems

Crucial objectives for militaries include protecting forces, increasing situational awareness, reducing soldiers' workload, and facilitating movement in challenging terrains. The integration of Robotics & Autonomous Systems (RAS) technologies enables militaries to achieve these objectives, control terrain, secure populations, and consolidate gains. Military RAS provides advanced capabilities to combat, reconnaissance, and support roles in warfare. Autonomous robots can perform various tasks, from defusing explosives to conducting search and rescue missions. These systems can operate independently or alongside human operators with the help of their advanced sensors and AI. In the future, RAS will focus on increased versatility, improved human-to-human interaction, and enhanced operational endurance, especially in hostile environments.

Advanced Defence Equipment

In response to emerging threats, more sophisticated defence equipment is being developed. This includes innovations from hypersonic flights and directed energy weapons to space militarization. Advanced defence equipment includes next-generation body armour, sophisticated missile defence systems, and resilient communication networks. Emerging technologies such as directed energy weapons (DEWs) and advanced electronic warfare systems are being made to counteract evolving threats and improve defence readiness. Such continuous advancements in materials science, electronics, and weapons systems will help maintain a technological edge over potential adversaries.

Big Data Analytics

In the evolving landscape of warfare, the role of information and its analysis is becoming increasingly crucial. Harnessing big data analytics, militaries unlock

insights from diverse data sources, gaining a strategic edge. Quantum computing, applied in cryptanalysis and simulations, aids informed decision-making. Efficient interpretation of data from the IoMT is another benefit of analytics. Predictive analytics not only deter threats but also enhance the safety and efficiency of perilous tasks. Anticipating potential threats and planning preventive measures is another key application of predictive analytics.

5G/6G Connectivity

In military operations, the importance of timely and appropriate information is paramount. Accelerating real-time decision support, 5G offers hyper-converged connectivity and secure data networks. This technology paves the way for new command-and-control applications and optimizes logistics. 6G is the sixth generation of cellular network technology; it will use radio frequencies to transmit data at faster speeds than previous generations. It is expected to be available in the early 2030s. 6G will make it possible to move freely in the cyber-physical continuum, between the connected physical world of senses, actions and experiences, and its programmable digital representation (Ericson, 2024)

Advancements in Manufacturing and Logistics

The defence industry is witnessing a paradigm shift towards advanced manufacturing techniques and innovative logistics solutions to enhance operational capabilities and efficiency. Additive manufacturing, commonly known as 3D printing, is revolutionizing defence production by enabling the fabrication of intricate and lightweight components with enhanced durability and performance. For instance, the application of 3D printing in producing aircraft and spacecraft parts reduces weight and material waste and accelerates the prototyping and production processes, enabling rapid iterations and customization. Adopting additive manufacturing technologies underscores the industry's commitment to agility, cost-effectiveness, and technological innovation in defence manufacturing. Moreover, advanced logistics innovations are pivotal in bolstering supply chain security and operational effectiveness within the defence sector. Defence companies can leverage technologies like blockchain to enhance transparency, traceability, and efficiency in their supply chain operations. For example, blockchain-enabled supply chain platforms provide real-time visibility into the movement of critical military assets, streamline procurement processes, and mitigate risks associated with disruptions. Integrating advanced logistics solutions optimizes inventory management and distribution and enhances operational readiness and responsiveness, ensuring seamless support for military missions and contingencies.

Adopting advanced manufacturing techniques also enables defence companies to stay competitive and agile in a rapidly evolving landscape. By embracing automation, robotics, and digital twin technologies, organizations can optimize production workflows, reduce costs, and accelerate the development

of next generation defence systems. For example, using robotics in assembly processes enhances precision, efficiency, and safety, leading to higher-quality standards and operational performance. The strategic integration of advanced manufacturing technologies reinforces the industry's resilience, adaptability, and innovation capacity, positioning defence firms for sustained growth and competitiveness in the global defence market. Future military technology is characterized by rapid innovation and integration across multiple domains. The top future military technologies discussed above will redefine defence and present new opportunities and challenges for forces worldwide. Staying informed about these trends is vital for understanding how modern warfare will evolve and for preparing for the next generation of military challenges.

Ramifications for India

The world is witnessing a rapid and unprecedented transformation in the character of warfare, driven by emerging technologies such as AI, robotics, cyber, space, quantum computing, directed energy weapons, and more. These technologies have the potential to create new domains of warfare, enhance existing capabilities, disrupt existing balances of power, and pose new challenges and threats to national security. The Indian Armed Forces are also on the path of modernization and advancement by integrating new weapon systems, platforms and sensors driven by emerging technologies and adopting new solutions to enhance their op preparedness and readiness to face any eventuality. The Indian Army celebrated year 2024 as the 'Year of Technology Absorption', reflecting how important it is to adopt the emerging technologies to remain future-ready. The military-technological landscape today is witnessing an exponential increase in the speed, lethality, and accuracy of kinetic instruments and the increased proliferation of technologies such as Quantum, AI, 5G, Semiconductors, 3D printing, Robotics, Deep Tech and nanotechnology.

Like any other developed countries, the Government of India has undertaken many initiatives for the development of Emerging and Critical Technologies to gain from the advantages these technologies accrue in enhancing National Security and propelling the economic growth as well as maintaining the balance of power. India has a vibrant ecosystem of startups, academia, industry, institutions, industry bodies, and research organizations like Defence and Research Development Organizations which is helping in the growth and adoption of these emerging technologies. India is now prepping for cutting-edge technologies, including 5G, AI, blockchain, AR and VR, machine learning & deep learning, robots, natural language processing, etc. These will be critical in the government and industry, for planning or decision-making, expediting development or analysing deployment, issue solving or product creation, detecting new trends or drawing out linkages and associations. The various ministries are at the forefront in terms of giving impetus to R&D and the adoption of these emerging technologies.

Initiatives by MeitY in Emerging Technologies

The Emerging Technologies Division of Ministry of Electronics and Information Technologies (MeitY) is responsible for fostering and promoting the utilization of cutting-edge technologies in India. The Emerging Technologies Division is supporting work for policy/strategy papers in the emerging areas like AI, AR/VR, IOT, blockchain, robotics, computer vision, drones, etc. (Ministry of Electronics, 2024a). The following initiatives have been taken by MeitY.

1 **Artificial Intelligence**: AI technology is being embraced by countries across the world, who are very keen on its potentially positive impact on the economy. Its proliferation is regarded as part of the Fourth Industrial Revolution. The Government of India has also envisioned supporting R&D and the adoption of such technologies. In view of the possible impact of AI on the economy and society and to come out with a policy framework on AI, MeitY constituted four committees on AI.
2 **Centres of Excellence for the Internet of Things (Gandhinagar, Bengaluru, Gurugram & Vizag)**: A Centre of Excellence (CoE) is a domain-specific specialized incubation facility for start-ups in the area of emerging technologies where the highest-standards and best-practices in terms of infrastructure, technology, leadership, mentoring, training, research & development, funding, networking for the given focus area are made available.

   MeitY, along with NASSCOM and state governments, has set up Centres of Excellence on the Internet of Things at Bengaluru, Gurugram, Gandhi Nagar and Visakhapatnam under the Digital India initiatives. In 2016, the first centre on IoT was established in Bengaluru with the support of the Government of Karnataka and NASSCOM. The key objective of these centres is to enable India to emerge as an innovation hub in IoT through the democratization of innovation and the realization of prototypes. Centres of Excellence on IoT connect various entities such as start-ups, enterprises, venture capitalists, government, and academia.
3 **Centre of Excellence on Virtual & Augmented Reality (VARCoE) at IIT Bhubaneswar**: With an objective to explore the opportunities in the niche area of VR & AR, Software Technology Parks of India, in partnership with MeitY, the Government of Odisha, IIT-Bhubaneshwar and a philanthropist, has established a Centre of Entrepreneurship for Virtual and Augmented Reality (VARCoE) at IIT-Bhubaneswar. Both VR & AR have massive innovation potential across a wide range of industries and research fields. These research and innovation activities are currently in domains across a range of industries including product and skill development, health and medical sciences, art and architecture, transport, construction, tourism, entertainment, education, and productivity software.
4 **Centre of Excellence on Gaming, VFX, Computer Vision & AI at Hyderabad**: This CoE was set up in collaboration with MeitY, STPI, the gaming industry and the Government of Telangana in January 2020 to provide resources

such as mentoring, technology support and funding for gaming, animation, VFX, computer vision and AI start-ups. It offers integrated programs, CVLAB and Game Lab for start-ups to scale up through its incubation facility. The center has been branded IMAGE. The IMAGE accelerator program includes premium plug-and-play co-working space for start-ups and offers access to the ecosystem which comprises IP owners, mentors, seed funding, investors and a platform to support a Go to Market strategy.

5 **Centre of Excellence on Blockchain Technology at Gurugram**: The STPI APIARY, a Centre of Entrepreneurship in Blockchain Technology, has been set up in collaboration with MeitY, STPI, the Government of Haryana, Padup Venture Private Limited, IBM, Intel, GBA and FITT in March 2020. This is an initiative to identify and evaluate promising start-ups in the field of Blockchain technology that will be hosted in the STPI Gurugram incubation facility.

6 **Design, Development, and Deployment of National AI Portal (INDIAai)**: The National AI Portal of India (INDIAai) is a joint venture by MeitY, NeGD and NASSCOM which has been set up to prepare the nation for an AI future. The portal has a plethora of research reports, datasets, case studies, educational institutes, courses, and articles about the ever-growing field of Artificial Intelligence.

7 **Proof of Concept (PoC) for AI Research Analytics and Knowledge Dissemination Platform (AIRAWAT)**: The Indian Government has initiated a project, AIRAWAT (AI Research, Analytics and Knowledge Dissemination Platform), to provide a common computing platform for AI research and knowledge assimilation. This AI computing infrastructure will be used by all technology innovation hubs, research labs, the scientific community, industry, start-ups and institutions under the overall umbrella of the National Knowledge Network. The PoC for AIRAWAT will be developed with 200 petaflops Mix Precision AI Machine which will be scalable to a peak compute of 790 AI petaflops.

8 **Formation of the Inter-Ministerial Committee for Development of Robotics Ecosystem in the country**: MeitY has constituted an inter-ministerial committee with secretaries from DoT, DSIR, DST, DPIIT and NITI Aayog as members and secretary, and MeitY as the convener. The committee will study the best practices on the role of government in supporting their domestic robotics industry & suggest ways forward to foster end-to-end ecosystem centred on robotics, including research, design, manufacturing, prototyping and utilization in manufacturing.

9 **Global Partnership on Artificial Intelligence**: The Global Partnership on Artificial Intelligence (GPAI) is an international and multi-stakeholder initiative to guide the responsible development and use of AI, grounded in human rights, inclusion, diversity, innovation, and economic growth. India is a founding member of GPAI, having joined the multi-stakeholder initiative on June 15, 2020. Since then, India has significantly contributed to GPAI goals and objectives and is working on various domestic initiatives

for the responsible development, deployment, and adoption of AI. As one of the largest Global South economies leading the AI race, India nominated itself for the position of incoming council chair of GPAI. India received more than two-thirds of first preference votes, and was therefore elected as the Incoming Council Chair in November 2022. India will serve as the Incoming Chair in 2023, then subsequently Lead Chair in 2024, and Outgoing Chair in 2025.

10 **India AI Report**: The Ministry of Electronics and Information Technology (MeitY) envisions the India AI programme as a mission-centric approach for leveraging transformative technologies to boost inclusion, innovation, and adoption for social impact. Pillars of India AI include AI in Governance, AI IP & Innovation, AI Compute & Systems, Data for AI, Skilling in AI, and AI Ethics & Governance. As part of building 'AI in India and AI for India', MeitY has formed seven expert groups to collaboratively brainstorm on the vision, objectives, outcomes, and design for each of India's AI pillars. The report comprehensively presents the objectives of the pillars of IndiaAI and recommends the next action items involved in harnessing the potential of AI for social development and achieving the goal of 'AI for ALL'.

11 **IndiaAI Mission**: The Government of India launched the IndiaAI Mission, a comprehensive national-level program, with the intention of democratizing and catalysing the AI innovation ecosystem in the country and ensure the global competitiveness of India's AI startups and researchers. The Mission aims to establish a robust AI ecosystem through strategic programs and partnerships across the public and private sectors. By democratizing computing access, improving data quality, developing indigenous AI capabilities, attracting top AI talent, enabling industry collaboration, providing startup risk capital, ensuring socially impactful AI projects and bolstering ethical AI, it will drive responsible, inclusive growth of India's AI ecosystem. The Mission will be implemented by 'IndiaAI' Independent Business Division (IBD) under Digital India Corporation (DIC) and it has the following components: IndiaAI Compute Capacity, IndiaAI Innovation Centre, IndiaAI Datasets Platform, IndiaAI Application Development Initiative, IndiaAI FutureSkills, IndiaAI Startup Financing, and Safe & Trusted AI. This Mission will propel innovation and build domestic capacities to ensure the tech sovereignty of India. It will also create highly skilled employment opportunities to harness the demographic dividend of the country and help India demonstrate to the world how this transformative technology can be used for social good and enhance its global competitiveness (Ministry of Electronics, 2024b).

Initiatives by the Ministry of Science & Technology

National Quantum Mission: The Union Cabinet approved the National Quantum Mission (NQM) on 19 April 2023 at a total cost of Rs.6003.65 crore from

2023–2024 to 2030–2031. Its aim was to seed, nurture and scale up scientific and industrial R&D and create a vibrant and innovative ecosystem in Quantum Technology (QT). This will accelerate QT-led economic growth, nurture the ecosystem in the country, and establish India as one of the leading nations in the development of Quantum Technologies & Applications (QTA) (Department of Science & Technology, 2023a). The Mission objectives include developing intermediate-scale quantum computers with 50–1000 physical qubits in 8 years in various platforms such as superconducting and photonic technology. Satellite-based secure quantum communications between ground stations over a range of 2000 kilometres within India, long-distance secure quantum communications with other countries, inter-city quantum key distribution over 2000 km as well as multi-node Quantum networks with quantum memories are also among the deliverables of the Mission. Mission Implementation includes the establishment of four Thematic Hubs (T-Hubs) in top academic and National R&D institutes in the domains:

1 Quantum Computing
2 Quantum Communication
3 Quantum Sensing & Metrology
4 Quantum Materials & Devices

The hubs will focus on the generation of new knowledge through basic and applied research and also promote R&D in areas that are mandated to them.

India Semiconductor Mission (ISM): The India Semiconductor Mission (ISM) was launched in 2021. The mission's goal is to establish India as a global leader in semiconductor design and electronics manufacturing. ISM is a specialized and independent scheme to enhance domestic manufacturing of chips in India. It is a very important initiative launched by the Government of India to boost the semiconductor chip and fab manufacturing ecosystem in the country. Its main objective is to make India a global hub for electronics and semiconductor chips manufacturing by creating the necessary infrastructure for semiconductor engineering, design, manufacturing, and research. It aims to establish a robust semiconductor and display ecosystem to position India as a global hub for electronics manufacturing and chip designing and research (Ministry of Electronics, 2024a). The ISM was launched in 2021 with a financial outlay of Rs. 76,000 crores under the control of the Ministry of Electronics and IT (MeitY), Government of India. It is an initiative under a comprehensive government-led program aimed at developing a robust sustainable semiconductor and display ecosystem in India. The programme, apart from its other provisions, provides financial help to chip manufacturing companies investing in semiconductors, display manufacturing, and design ecosystem (Testbook, 2024)

5G: Telecom Regulatory Authority of India (TRAI) has recently issued a Consultation Paper on "Digital Transformation through 5G Ecosystem". The objective of this consultation paper is to identify the policy challenges and

suggest the right policy framework for faster adoption and the effective utilization of new technologies for the holistic and sustainable development of the economy driven by the 5G ecosystem. India is undergoing a rapid digital transformation that is reshaping its economy and society. Fast and reliable mobile communication technologies are helping the Government to realize the objectives of the Digital India programme. It is providing a boost to the country's economy and empowering the citizens through services like unified payment interface (UPI) and several other innovative G2B and G2C applications. With the advent of technologies such as 5G, the IoT, AI, AR/VR and the Metaverse, India is poised to unlock new opportunities for growth and innovation (Ministry of Communications, 2023).

Drone Manufacturing: The Government of India has several initiatives to support the drone manufacturing industry, including the Production Linked Incentive (PLI) scheme, the Drone Shakti scheme, and the Telangana Drone City (Government of Telangana, 2024). An incentive of Rs. 120 crores have been provided for Indian manufacturers of drone and drone components under the PLI Scheme. The Production-Linked Incentive (PLI) Scheme for drones and drone components has been notified on 30 September 2021 to promote the manufacturing of drones and drone components in India (PIB, 2021) The government has also released the Drone Rules, 2021, which aim to reduce the paperwork and costs involved in owning, manufacturing, and operating drones (PSA Content Desk, 2021).

Deep Tech: Deep Technology refers to innovations founded on advanced scientific and technological breakthroughs. Due to their disruptive nature, they have the potential to solve India's most pressing societal issues. The draft *National Deep Tech Startup Policy (NDTSP)* is strategically formulated to stimulate innovation, spur economic growth, and promote societal development through the effective utilization of deep-tech research-driven innovations. This initiative centralizes on bolstering deep-tech startups, thereby solidifying India's financial stability and stimulating the transition towards a knowledge-centric economy, consequently augmenting India's overall productivity. NDTSP aims to harness the transformative potential of technological advancement across diverse sectors, serving as a catalyst to stimulate ripple effects throughout the economy and laying the groundwork for the creation of new industries. This policy aims to significantly strengthen India's capabilities and enhance global competitiveness (PSA Content Desk, 2024)

Anusandhan National Research Foundation (ANRF): Anusandhan National Research Foundation (ANRF) has been established under the Anusandhan National Research Foundation (ANRF) 2023 Act. The ANRF aims to seed, grow and promote research and development (R&D) and foster a culture of research and innovation throughout India's universities, colleges, research institutions, and R&D laboratories. ANRF will act as an apex body to provide high-level strategic direction of scientific research in the country according to the recommendations of the National Education Policy (NEP). With the establishment of ANRF, the Science and Engineering Research Board

(SERB) established by an act of Parliament in 2008 has been subsumed into ANRF. This body will forge collaborations among the industry, academia, and government departments and research institutions, and create an interface mechanism for the participation and contribution of industries and State governments in addition to the scientific and line ministries (Department of Science & Technology, 2023b).

iCET Initiative: The United States–India Initiative on Critical and Emerging Technology, or iCET, is a collaborative framework established by the United States and India to enhance cooperation in developing fields of technology. The US president and the Indian prime minister announced the US–India initiative on Critical and Emerging Technology (iCET) in May 2022 in order to elevate and expand strategic technology partnership and defence industrial cooperation between the governments, businesses, and academic institutions of the two countries. The United States and India affirm that the ways in which technology is designed, developed, governed, and used should be shaped by their shared democratic values and respect for universal human rights. Both governments are committed to fostering an open, accessible, and secure technology ecosystem, based on mutual trust and confidence, which will reinforce shared democratic values and democratic institutions (Chaudhuri & Bhandari, 2024)

Initiatives by Ministry of Defence Innovations for Defence Excellence (iDEX): The scheme, launched by the Hon'ble Prime Minister in 2018, aims to foster innovation & technology development in defence and aerospace by engaging innovators & entrepreneurs to deliver technologically advanced solutions for modernizing the Indian military. The iDEX provides a collaborative platform for stakeholders to co-create and develop innovative defence technologies. The iDEX runs challenges for Indian startups, MSMEs, and individual innovators, including the Defence India Startup Challenge (DISC), Open Challenge, Thematic Open Challenge and Advancing Defence Innovation Acing Development of Innovative Technologies with iDEX (ADITI) Challenge.

iDEX aims at the creation of an ecosystem to foster innovation and technology development in Defence and Aerospace by engaging industries, including MSMEs, start-ups, individual innovators, R&D institutes & academia and providing them with grants/funding and other support to carry out R&D, which has good potential for future adoption to serve Indian defence and aerospace needs. iDEX will be funded and managed by a 'Defence Innovation Organization (DIO)' which has been formed as a 'not for profit' company as per Section 8 of the Companies Act 2013 for this purpose, by the two Defence Public Sector Undertakings (DPSUs), namely, HAL & BEL. iDEX will function as the executive arm of DIO, carrying out all the required activities while DIO will provide high level policy guidance to iDEX (Innovation for Defense Excellence, 2018)

These initiatives taken by the Government of India, amply supported by premier academic institutions, research organizations, industrial bodies, industry & vibrant startup ecosystem, and apart from international collaboration,

will boost the research & development in the domain of emerging and critical technologies. In addition, these initiatives will help in the production of world-class indigenous products which are needed by our critical sectors for their security. The adoption of these technologies will not only help in enhancing our national security but also contribute to the economic growth of our nation. The major beneficiary of the development of emerging & critical technologies is the military of the nation, which requires cutting-edge technologies in their mission-critical systems for enhancing their war waging capabilities and create deterrence.

Fitment Required by Indian Armed Forces

As emerging technologies reshape warfare, India must adapt its military strategies accordingly. This involves not only incorporating new technologies into their arsenal but also rethinking traditional concepts of deterrence and warfare. The Indian military is tasked with developing a comprehensive strategy that integrates these technologies into its operational framework while addressing the unique challenges posed by its adversaries. India's defence preparedness requires a focus on the indigenous development of advanced military technologies. The country has made strides in enhancing its defence manufacturing capabilities but still relies on foreign technology for many critical systems. A concerted effort to develop homegrown solutions will be essential for maintaining strategic autonomy and ensuring readiness against emerging threats. The deployment of autonomous weapons raises ethical questions regarding accountability and the potential for unintended consequences in warfare. As India integrates these technologies into its military strategy, it must also engage in discussions about the ethical implications of their use, ensuring compliance with international humanitarian law (Allenby, 2013).

Attaining Aatmanirbharta (Self-Reliance)

Factoring the emerging technologies in developing our own weapon systems not only enhances our war-waging capability but also allows us to march towards Aatmanirbhar Bharat, the dream of our PM. A few of the remarkable feats achieved so far in making Bharat, a powerful influential nation, are as follows.

Tejas: The HAL Tejas Mark 2 or Medium Weight Fighter (MWF) (Krishnan, 2020a) is an Indian single-engine, canard delta wing, multirole combat aircraft designed by the Aeronautical Development Agency (ADA) in collaboration with the Aircraft Research and Design Centre (ARDC) (Krishnan, 2020b) of Hindustan Aeronautics Limited (HAL) for the Indian Air Force (IAF). It is a further development of the HAL Tejas, with an elongated airframe, a closely coupled canards, new sensors, and a more powerful engine. The roll-out of the first prototype is expected by 2025, with the first flight by 2026 and mass

production by 2029. Developing our own aircraft like Tejas and its variants are a big step towards Aatmanirbharta.

Anti-satellite missile (ASAT): Mission Shakti' was the country's first ever Anti-Satellite (ASAT) Missile Test. It was successfully conducted on 27 March 2019 from Dr AP J Abdul Kalam Island in Odisha, where a fast-moving Indian orbiting target satellite in Low Earth Orbit (LEO) was neutralized with pin-point accuracy. This was a highly complex mission, conducted at extremely high speed with remarkable precision. The successful conduct of Mission Shakti made India the fourth nation in the world with the capability to defend its assets in outer space (Ministry of Defence, 2020).

Hypersonic Missile: India conducted its first hypersonic missile test in November 2024. However, India has been working on hypersonic technology for nearly two decades. This puts India in an intensifying global hypersonic missile arms race where the US, Russia, and China are the front-runners (Jalil, 2025). India is the first country to develop a long-range hypersonic missile able to travel more than eight times the speed of sound. According to defence scientists, it is a game-changer in global defence technology which no other countries have (Rout, 2024).

Indian Navy Commissions INS *Surat*, INS *Nilgiri* and INS V*agsheer*: Recently three frontline vessels were commissioned into the Indian Navy, namely: the destroyer INS *Surat*, the last of the four Visakhapatnam-class stealth guided-missile destroyers; the frigate INS *Nilgiri*, the lead ship of a new class of seven stealth guided-missile frigates being built under Project 17 Alpha; and the submarine INS *Vagsheer*, the sixth and last of the first batch of the Kalvari-class diesel-electric attack submarines. These few stated examples clearly indicate how the induction of state-of-the-art weapon systems and platforms laced with cutting-edge technologies is providing the Indian military with a much-needed boost in its arsenal, enhancing operational preparedness and war-waging capabilities. The integration of emerging and critical technologies has played a key role in enhancing the speed, accuracy and lethality of the Indian armed forces, and indigenous development has increased our self-reliance.

Bhargavastra: India successfully tested "Bhargavastra", an indigenous Counter Drone System with guided micro-missiles developed by Economic Explosives Ltd (EEL). The system, featuring both hard-kill and soft-kill capabilities, can detect large drones at 10 km and small ones at 6 km (TOI Business Desk, 2025). The system functions across varied terrain up to 5000 m altitude and can neutralize drone swarms.

Conclusion

Emerging technologies are fundamentally altering the nature of warfare, presenting both opportunities and challenges for nations around the globe. Adoption of emerging technologies will help our military to reduce our OODA (Observe, Orient, Decide, Act) and increase it for the adversary, which

is particularly crucial in war. This helps in aligning our weapon systems quickly to neutralize the enemy through swift decision-making by the military commander. For India, embracing these changes is crucial to maintaining its strategic edge in a rapidly evolving security environment against the backdrop of two ongoing wars. By investing in technological advancements and adapting its military strategies accordingly, India can enhance its defence capabilities and effectively respond to the complexities of modern warfare while navigating the ethical dilemmas that accompany these innovations. Although emerging technologies enhance efficiency, they also introduce new risks. Organizations must prioritize cybersecurity to mitigate these threats. Additionally, India's rapid digitization has led to vulnerabilities in its technical infrastructure, resulting in an increase in cyber-attacks. Therefore, it is imperative that when developing any new product, the concept of "Secure by Design" principle must be kept in mind by all the manufacturers to reduce the vulnerabilities, especially in the critical systems. By designing and developing our own mission critical systems, India is trying to achieve true "Aatmanirbharta", which is a key requirement for our nation becoming the "Viksit Bharat" dream of all Indians and our prime minister.

References

Allenby, B. (2013). The implications of emerging technologies for just war theory. *Public Affairs Quarterly*, *27*(1), 49–67. http://www.jstor.org/stable/43574496

An Introduction to the Building Blocks of Global Trends. Office of the Director of National Intelligence—Global Trends.(2021, March). https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield

Anand, V. (1999, April). Impact of technology on conduct of warfare. *Strategic Analysis*:*A Monthly Journal of the IDSA*, *XXIII*(1). https://ciaotest.cc.columbia.edu/olj/sa/sa_99anv02.html

Bommakanti, K., Vats, A., Nachiappan, K., Mohan, S., & Joshi, Y. (2024, May 10). *Emerging Technologies and India's Defence Preparedness*. orfonline.org. https://www.orfonline.org/research/emerging-technologies-and-india-s-defence-preparedness/

Chaudhuri, R., & Bhandari, K. (2024, October 23). *The US–India Initiative on Critical and Emerging Technology (ICET) from 2022 to 2025: Assessment, Learnings, and the Way Forward| Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2024/10/the-us-india-initiative-on-critical-and-emerging-technology-icet-from-2022-to-2025-assessment-learnings-and-the-way-forward?center=india&lang=en

Cristian, B. (2015). The evolution of warfare from Classic to hybrid. *Strategic Impact; Bucharest*, No. 55, 57–66. https://www.proquest.com/docview/1731537073

Department of Science & Technology (DST). (2023a). *National Quantum Mission (NQM)*. वज्ञिान एवं प्रौद्योगकी वभिाग. https://dst.gov.in/national-quantum-mission-nqm/

Department of Science & Technology (DST). (2023b). *Anusandhan National Research Foundation (ANRF)*. Government of India. https://dst.gov.in/anusandhan-national-research-foundation-anrf

Dwivedi, G. G. (2023). *Changing Nature of Limited Wars: Impact of Technology*. https://www.usiofindia.org/publication-journal/Changing-Nature-of-Limited-Wars-Impact-of-Technology-and-Ramifications.html

Ericson 6G – follow the journey to the next generation networks. Blog Post (2024). https://www.ericsson.com/en/6g

Government of Telangana. (2024, May 23). *Drones Framework*. Department of Information Technology, Electronics & Communications. https://it.telangana.gov.in/initiatives/drones/

India Semiconductor Mission & Chip Manufacturing in India. Testbook. (2024, September 21). https://testbook.com/editorials/india-semiconductor-mission-chip-manufacturing

Innovation for Defense Excellence. iDEX. (2018). https://idex.gov.in/

Jalil, G. Y. (2025, February 5). *Issue Brief on "India Joins the Global Hypersonic Missile Race"*. Institute of Strategic Studies Islamabad. https://issi.org.pk/issue-brief-on-india-joins-the-global-hypersonic-missile-race/

Junaid, K. (2024, June 11). *Emerging Technologies and Their Impact on Warfare*. Modern Diplomacy. https://moderndiplomacy.eu/2024/06/11/emerging-technologies-and-their-impact-on-warfare/

Krishnan, M. A. (2020a, February 3). *India's Medium Weight Fighter Set to Fly into Detail Design Phase*. OnManorama. https://web.archive.org/web/20200203182308/https://english.manoramaonline.com/news/nation/2020/02/03/india-defence-expo-medium-weight-fighter.html/

Krishnan, M. A. (2020b, December 10). *With Expected 83 Tejas MK1A Orders, ARDC Shapes India's Upgraded Fighter*. OnManorama https://www.onmanorama.com/news/india/2020/08/05/with-expected-83-tejas-mk1a-orders-ardc-shapes-india-upgraded-fi.html/

Ministry of Communications. (2023). *TRAI Issues Consultation Paper on "Digital Transformation through 5G Ecosystem*. https://pib.gov.in/PressReleasePage.aspx?PRID=1962170/

Ministry of Defence. (2020). *Raksha Mantri Shri Rajnath Singh Unveils A-Sat Missile Model in DRDO Bhawan*. https://pib.gov.in/PressReleasePage.aspx?PRID=1671442/

Ministry of Electronics. (2024a). *Ai & Emerging Technologies Group*. https://www.meity.gov.in/emerging-technologies-division

Ministry of Electronics. (2024b). *India Semiconductor Mission*. https://www.ism.gov.in/

New Military Technology Trends (2024–2025). Oledcomm. (2024, October 14). https://www.oledcomm.net/blog/new-military-technology/

PIB. (2021, December 9). *Incentive of Rs. 120 Crore Has Been Provided for Indian Manufacturers of Drone and Drone Components under PLI Scheme*. Ministry of Civil Aviation. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1779782

Press Trust of India. (2024, April 24). The Chief of army staff explains how technology is emerging as a new strategic arena of competition. *Deccan Herald*. https://www.deccanherald.com/india/chief-of-army-staff-explains-how-technology-is-emerging-as-a-new-strategic-arena-of-competition-2992269

PSA Content Desk. (2021). Revamped drone policy provides new opportunities for businesses and end users. *Principal Scientific Adviser*. https://www.psa.gov.in/article/revamped-drone-policy-provides-new-opportunities-businesses-and-end-users/3583/

PSA Content Desk. (2024, May 9) *NDTSP: Transforming India through Deep Tech Innovation*. https://www.psa.gov.in/deep-tech-policy

Rajagopalan, R. P., & Patil, S. (2024, February 12). *Future Warfare and Critical Technologies: Evolving Tactics and Strategies*. orfonline.org. https://www.orfonline.org/research/future-warfare-and-critical-technologies-evolving-tactics-and-strategies/

Report World Economic Forum. (2024, June 25). *Top 10 Emerging Technologies of 2024*. https://www.weforum.org/publications/top-10-emerging-technologies-2024

Reuters. (2024, June 11). *Ukraine Names Commander of Drone Systems*. https://www.reuters.com/world/europe/ukraine-names-commander-drone-systems-2024-06-10/

Rout, H. K. (2024, December 1). *India First to Develop Long-Range Hypersonic Missile: Defence Experts*. The New Indian Express. https://www.newindianexpress.com/states/odisha/2024/Dec/01/india-first-to-develop-long-range-hypersonic-missile-defence-experts/

Seligam, L., & Berg, M. (2020, December 12). A $2m missile vs. a $2,000 drone: Pentagon worried over cost of Houthi attacks. https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480

Sengupta, A. (2021, March 20). *Evolution of Warfare with Technology*. Defence Research and Studies. https://dras.in/evolution-of-warfare-with-technology/

Sharma, A. (2023, October 4). *Emerging Technologies and the Future of the Indian Army*. DefenceXP. https://www.defencexp.com/emerging-technologies-and-the-future-of-the-indian-army/#google_vignette

Singh, V. P. (2024, November 12). *Impact of Niche Technologies on Joint Warfighting*. CENJOWS. https://cenjows.in/impact-of-niche-technologies-on-joint-warfighting

TOI Business Desk. (2025). *India Successfully Tests Indian Army's First "Bhargavastra" Counter-Drone Micro Missiles - Details Here*. The Times of India. https://timesofindia.indiatimes.com/business/india-business/india-successfully-tests-indian-armys-first-bhargavastra-counter-drone-micro-missiles-details-here/articleshow/117262056.cms

15 India's Quest for Hybrid Warfare
Strategic Implications

Bharti Das and Uday Pratap Singh

Introduction

Hybrid warfare is one of the most complicated, multifaceted forms of conflict, combining the destructive capability of conventional war with the characteristics of secrecy and unpredictability brought about by irregular tactics. This type of contemporary warfare uses cutting-edge technologies, like cyber operations and information warfare, to accomplish strategic objectives. It combines traditional and non-traditional strategies to increase power, influence, and harm with the actual operations taking place even under the pretense of a tranquil period, hybrid warfare threatens much of society, in contrast to the more conventional wars that had characterized battlefields. Hybrid warfare uses techniques including terrorism, cyberattacks, legal manipulation, and planned public disturbance, but because it involves sophisticated doctrines and innovative strategies, it appears to be very similar to peace. India is moving forward and facing issues related to hybrid warfare. In order to combat the threat and strengthen national security for long-term sustainability, this chapter examines a comprehensive and realistic strategy.

Since its independence in 1947, India has been threatened by hybrid warfare; however, this situation was brought about by Pakistan's persistent employment of state-sponsored terrorism and disruptive tactics, and it still exists today. China is another country that has adopted hybrid warfare, since it has also made its defence forces upgradeable to better suit the dynamics of modern conflicts. These dangers range from cyberattacks and unconventional warfare to terrorism aimed at undermining India's social and political stability. In times of peace, these strategies remain unchanged during conflicts, however, their use escalates. Because of Pakistan's protracted proxy war, terrorism was officially created as an aggressive tactic. Given the rapidly evolving nature of these threats, India needs to strategically realign itself to create a more effective and precise defence system. India's first and former CDS, General Bipin Rawat, offered a perspective on the complexity of future conflict and the degree of improved operational readiness along India's frontiers. For national security against hybrid threats, India must integrate technology, intelligence-driven reaction, and additional interagency collaboration.

DOI: 10.4324/9781003633204-18

Military strategist Frank G. Hoffman summarizes the general consensus in defining hybrid warfare as a fight in which states and non-states apply conventional armed forces, irregular operations, terrorism, and disruptive technologies for the destruction of political and social fabrics. Such approaches might be used together with one another or might be integrated into one plan to harm the victim country. Thus, an important feature of hybrid warfare would be the manner in which this could affect the psychological resilience rather than just a nation's infrastructure, thus breaching the will to resist. Hybrid warfare in the present interdependent world thrives on globalization and feeds upon the immediacy of information diffusion for the manipulative purposes of public perception to sow instability and uncertainty at home and abroad.

Acknowledging these changing threats, the Pentagon's 2006 Quadrennial Defence Review noted that "irregular warfare has emerged as the central form of conflict in the post-9/11 world." Such a recognition signals a strategic shift toward underlining the increasing relevance of hybrid warfare in modern military doctrine. Hybrid warfare is one where traditional distinction between conventional, irregular, and cyber conflicts tend to blur and blur into an increasingly complex and unpredictable security environment. The adjustment key to an effective response to challenges created by hybrid threats for India lies in the adjustment of strategy in defence.

This chapter examines the nature and evolution of hybrid warfare from the Indian perspective so as to propose a solution towards countering hybrid threats. Hybrid forms of war have been studied in depth for many decades, but it seems to be an area where no research has looked into the matter in relation to the Indian perspective. This study tries to analyze strategic dynamics in hybrid warfare and seek measures that can be undertaken by India to increase its preparedness against such multifaceted threats. Hybrid warfare would be targeting strategic long-term gains, rather than short-term tactical wins in which a hybrid threat is valid and operational until decisively degraded. Hence, the Indian response would need to evolve beyond military-level actions into disassembling the socio-political structures that provide a fertile ground and feeding environment for the hybrid threat. Hybrid warfare is the reality for today as well as tomorrow, and hence becomes a big challenge in itself for the future. Thus, the most critical thing that India needs to do is to continually review its defence strategy, making it capable of a response to threats under the genre of the unconventional. In the long term, it would require a good understanding of hybrid warfare's complexity, coupled with an evolving response framework which is simultaneously both comprehensive and fairly versatile.

Evolution of Hybrid Warfare

Hybrid warfare has become increasingly relevant in modern conflict scenarios, but its exact origin and definition remain a subject of ongoing debate (Bjerregaard, 2012). While there is no universally accepted definition, the evolution of the

term, and its implications in the military strategy landscape, are critical to understanding its significance. This section explores the history of hybrid warfare, its definition, and the challenges in response to this new form of warfare. The term "Hybrid Warfare" was first coined by US Marine Corps Lieutenant Colonel Frank G. Hoffman, 2006 (Hoffman, 2007). Hoffman himself gives credit to the origins of the concept to Robert G. Walker's, 1995 thesis, which documented a series of low-intensity operations executed by the US Marines. Hoffman coined the term "complex irregular warfare" in 2006, as he had first discussed this idea with US Marine Corps General James Mattis & Hoffman, 2005 opinion piece published in the United States Naval Institute Proceedings Magazine (Mattis & Hoffman, 2005).

In 2007 Hoffman formally defined hybrid warfare in rigorous academic terms: the combination of several methods of warfare. He later described it as including conventional military capabilities, irregular tactics, terrorism (Aronsson, 2019), indiscriminate violence, coercion, and criminal disorder. It was this definition that provided a foundation for scholars and militaries to build on and refine later. Hoffman and others would modify this definition as time went by, but for most, 2007 will mark the origin (Hoffman, 2007). The hybrid warfare debate also opened the venue to significant criticisms. For instance, the argument that Hybrid Warfare is a Revolution in Military Affairs, or that it is a totally new form of warfare (Bjerregaard, 2012). In a broader analysis, in the *Oxford Handbook of War*, Rob de Wijk summed up a fair amount of debate until that date and also pointed out that hybrid warfare is continuously advancing from generation to generation from the traditional military paradigms (Wijk de, 2012). The evolution also continued well in the 2010s; however, by 2015, notable scholars Tenenbaum (2015) and Thornton (2015) updated significant perception regarding the relevance of hybrid warfare. Although the concept of hybrid warfare does have a fuzzy definition, several commonly accepted features do exist, particularly between scholars and military experts. To put it bluntly, hybrid warfare refers to the combined employment of conventional and unconventional methods and tactics in their use, more often by both state and non-state actors. Other essential features are outlined below:

- Non-Standard and Complex Adversaries: Hybrids can, in fact, be either a state or a non-state adversary. Their propensity to operate with traditional as well as irregular channels makes hybrids very adaptive entities. Shifting tactics to the point of trying to exploit every weakness of a given opponent forms part of conventional strategy employed by such adversaries Caliskan, 2019).
- For quite some time, hybrid warfare has been defined as the combination of traditional and non-traditional forms of warfare (Bjerregaard, 2012). For example, hybrid forces include conventional warfare in addition to the irregular forms of warfare, which are guerrilla warfare, insurgency, and terrorism. Such a diversified nature of warfare makes hybrid adversaries impossible to predict or counter.

- Technological Innovation and Disruption: Hybrid actors are fairly well prepared through the exploitation of advanced weapons systems and emerging technologies. Cyber warfare and unmanned aerial vehicles, as well as other disruptive technologies, provide for such actors technological superiority to impact military and civilian infrastructure (Pandit, 2018).
- Mass Communication and Psychological Operations: One important hybrid warfare component is the ability to shape public opinion and manipulate the information environment. Hybrid adversaries, most often, employ mass communication networks to spread propaganda recruit supporters and create confusion in enemy populations (Sloan, 2017). Fake news social media manipulation, and other means of disinformation, are core components of this strategy (Gompert, 2007).
- Multiple Fronts: Hybrid warfare possesses three different battlefields: the conventional military battlefield, the local population within the conflict zone, and the international community. In this way, hybrid actors create multiple fronts with which to simultaneously war on their opponents.

Despite its wide usage across military and academic circles, the term hybrid warfare can still not be understood universally. The abstractness of the concept also means that it is quite easily applied as a "catch-all" term for all sorts of non-traditional or irregular threats. It has thus attracted an assortment of different interpretations and much debate over scope and implications. One of the greatest challenges in setting a definition to hybrid warfare is that there is no clear line of demarcation when it comes to war and peace. Much of hybrid warfare often occurs below the threshold of conventional conflict, where military and non-military lines become very blurred. The complexity adds to the difficulty of placing hybrid warfare into one or other of these categories of war or tactics in an ongoing conflict.

In hybrid warfare, the traditional response of military appears not to work. Here, the mobilization of hard power or military power would not help; the latter has exercises with unconventional or unorthodox forms. Thus, adversaries often take advantage of this confusion by taking place in those areas where apparent or traditional military powers are confined or nullified. This is also a testimony to one of the greatest features of hybrid warfare: its flexibility. Hybrid actors are less restricted by formal military structures, and they display higher levels of innovation and flexibility than their traditional peer militaries. The conventional forces' structured approach towards warfighting makes it difficult for them to adapt to the fluid nature of hybrid warfare. Hybrid warfare is a new pattern for conducting armed conflict, connecting conventional military capabilities with non-regular tactics and cyber operations.

The Hybrid Threats to India

The threats against India are multilayered, consisting both of internal and external elements involving a mix of state and non-state actors. The Indian

security environment is complex, comprising multiple dimensions that involve traditional and modern warfare along with unconventional and asymmetric tactics (Tenenbaum, 2015). This dynamic has given rise to what is more generally known as "hybrid threats," which refers to the combining of several military and non-military tactics directed at undermining a country. These hybrid threats against India are nothing new, but they have been in development for some time; the problems become more intricate and sophisticated with each passing year.

Internal and External Hybrid Threats

India faces a number of internal insurgencies, including separatist movements in Kashmir and Naxalism (Niruthan, 2016). On the outside, it is more seriously threatened by its neighbors, especially China and Pakistan. For many years, these outside parties have been using hybrid strategies against India, which has exacerbated regional instability in addition to stoking domestic problems. For the area, hybrid dangers are not a recent development. India has already seen certain cases in which hybrid warfare methods were used before the phrase became popular in Western military discourse (Tenenbaum, 2015). The Liberation Tigers of Tamil Eelam (LTTE) from Sri Lanka are a great example of just such a non-state player. They were able to combine irregular insurgent tactics with traditional military assets, such as the deployment of an army, a navy, and an air force. Additionally, The LTTE is a prime example of a hybrid danger since it also maintained a global propaganda network (Exum, 2006). Another significant incident in the neighborhood that can be taken as one of the first instances of hybrid warfare in modern times was the Soviet–Afghan conflict of the late 1970s and early 1980s. This is the conflict within India's neighborhood, which comprised both conventional and unconventional methods of war and, in turn, paved the way for future hybrid conflicts in the region.

The Role of Pakistan and China in Hybrid Threats

For decades, Pakistan has been a core player in hybrid warfare against India (Thornton, 2015). Irregular forces and terror outfits targeting India, particularly for the destabilization of Kashmir, have been integral parts of these strategies and have carried out several attacks into the region from time to time through indirect methods such as terror, psychological attacks, and fake news in order to gain an upper edge. Though these groups have not possessed state-like destructive power to date, in future, as a result of scientific progress, they may assume it (Livermore, 2017). Hence, this problem has an absolute likelihood of also becoming more complex for India. China's involvement in hybrid warfare against India is also increasingly significant. It exercises asymmetric pressure against India through its relationship with Pakistan. It appears that China has been involved in supporting insurgent movements in the northeast of India and the Naxal movement, further complicating India's security

challenges (Ahluwalia & Kapoor, 2019). Moreover, hybrid warfare capabilities in China are one of the formidable threats to regional stability, in addition to security for India. Standoffs with India's Intelligence Bureau, transgressions, intrusions, increasing assertiveness on the political and military fronts, intrusions into the Indian Ocean, threatening island territories, economic colonization through debt traps (Sinha, 2016), cooperation with like-minded nations, and a general mindset of "coercive gradualism" are all part of China's hybrid war strategy (Kumar, 2023).

The Taliban is another emerging hybrid threat to India: In light of the evolving situation in Afghanistan, this is likely to continue. Should the Taliban gain full control over Kabul, the Pakistanis would naturally use this opportunity to leverage the Taliban's proclivities for training and planning attacks against India, especially in Kashmir. Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM), being state-sponsored weapons of Pakistan, can be allowed to operate openly from Afghanistan, further escalating the threat against India's national security (Dheeraj, 2016). In addition to these external challenges, there is an internal challenge that has begun to grow in India very recently: radicalization. The "fourth front" of hybrid warfare involves the manipulation of religious or ethnic identities inside the country through both state and non-state actors. Radicalization has been used to incite violence and create an unstable environment and is one of the most evil forms of war, as it attacks social unity from within.

Non-Traditional Hybrid Threats

The nation continues to face some hybrid challenges from non-traditional sources in addition to regular military operations and resurgence. Like smuggling, the proliferation of counterfeit notes, and restricting trade through certain protectionist tendencies can destabilize the economy in the nation; China and Pakistan have been responsible for such manoeuvres whereby they have wielded these forms of activities with the intention of undermining India's economic strength and thwarting its growth at any given juncture of time. Another hybrid threat is water-related warfare (Chellaney, 2017); that includes any means which might create a shortage or oversupply of the commodity resulting in floods, and so on. These might not only aggravate the existing environmental problems but also help create humanitarian crises, and fuel conflict in the country (Mazarr, 2015).

Hybrid Warfare and National Security

Any hybrid threats would have to be understood within India's national security paradigm. Indeed, security for India is organically tied in with the larger contours of its national politics and culture. There is an unbridgeable correlation between national security and political or social stability plus economic growth that must characterize these goals, having both internal as well as hybrid

and other foreign external factors contributing to such potential and realized imperatives. National security in India requires a consideration of the larger political and cultural environment. This will mean understanding perceptions held by neighboring countries and the global superpowers at large, as well as how such perceptions might inform their approaches to India. India needs a holistic approach towards security policy in order to tackle the complex nuances of hybrid warfare and securing India's interests in an increasingly connected and unstable world. In its history, India has responded to hybrid threats, but this was usually as a reaction; new developments make it harder to adopt such an approach now. Of late, more commonly, India has used defensive measures, such as the surgical strike it recently took against terrorist camps in Pakistan and the way China has strategically encircled the country. All of these measures are part of a general plan of containment and neutralization of hybrid threats before they grow into bigger incidents. India's socio-political texture of diverse ethnic, religious, and cultural streams can complicate the security strategy of the country. The practice of making the national security robust should involve integrating the cultural and civilizational considerations with practical measures of security. All this requires successful leadership at different levels, as well as a commitment to social justice, national stability, and world peace.

There have always been hybrid threats against India, and these have continued to evolve. Today, the traditional threats remain an old threat by Pakistan and China. In addition, the emerging threats of radicalization and environmental warfare challenge India on all fronts. Hybrid threats demand a comprehensive national security approach that is required to address unique cultural, political, and institutional realities of India.

Hybrid Response: A Strategic Framework for India

Hybrid warfare is the outcome of a combination of conventional military forces, irregular tactics, cyber strategies, and information campaigns in a complex matrix. Hybrid warfare has emerged as a dominant challenge for nations everywhere. In terms of the heterogeneity of socio-political characteristics and strategic vulnerabilities, India's response must reflect the change in the nature of this threat. Hybrid warfare is not a simple military challenge; rather, it is a multidimensional one, demanding a full, coordinated national strategy (Hoffman, 2010). Obviously, hybrid responses are needed as such warfare challenges the very foundation of a state by exploiting fault lines within a country, manipulation through psychology, and indirect actions to destabilize a nation. Hybrid warfare is also characterized by its inherent uncertainty. When a conventional army or other large groups of troops appear to be engaged in traditional warfare, the enemy's aims become immediately apparent. In the dark, hybrid warfare flourishes. Cyberattacks, economic pressures, media campaigns, and irregular combatants are just a few examples. As a result, early detection of the threat is difficult. The enemy is active on all fronts: political, social, economic, external, and internal.

For India, a nation torn between the threat of China and Pakistan on the one hand, and domestic insurgencies and radicalism on the other, hybrid conflicts are an inevitable part of life. The national security strategy needs both defensive and offensive measures that uphold state integrity, which means bolstering the nation's institutions. Hybrid warfare attacks a state at a level of attacking its internal coherence, and there is thus an obligation on states to deny a terrorist space, denying them to utilize the inner cracks of a country. Countering such a threat begins by consolidating vulnerabilities, preventing state implosion by undermining the country's internal mechanisms, and using all levels of government in tandem – that is, preventive as well as responsive measures (Smith, 2006).

A National Strategy for Hybrid Warfare

Hybrid warfare needs to be accepted as a permanent feature of India's security environment. Here, the threat itself is a challenge: being hybrid, and therefore requiring a response that must be integrated and multidimensional. Undeniably, the military will have to form the core of any national strategy against this hybrid menace; however, it is the threat that is most unlikely to be answered solely in terms of conventional military capability. Hybrid threats apply none of the traditional rules of engagement; lines between war and peace blur, and there are multiple means of attack, which call for a much more subtle strategy. The doctrine on military strategy needs to emerge or surpass traditional warfare and to evolve in order to accommodate counterinsurgency techniques, cyber warfare, and information warfare. In this regard, there is a need to develop new doctrine on integrated action based on the acknowledgment of the complications of hybrid war. A key element of this strategy will involve the restructuring of forces, special training, and the development of specialized equipment tailored to counter the diverse elements of hybrid warfare. The military needs to prepare to fight on multiple fronts and integrate both combat and non-combat forces in order to be able to respond to the entire spectrum of hybrid threats.

Intelligence agencies play a very crucial role in finding and countering hybrid threats. The threat usually starts with the mindset of the population and later translates into the physical world. Hybrid warfare takes advantage of social, cultural, and economic tensions within a society, normally based on radicalization, misinformation, and foreign manipulation. In such terms, the way forward to counter hybrid threats is for intelligence agencies to realize and map the human terrain in order to understand the social and cultural fault lines they might be used against (Johnson, 2019). Hybrids need intellectuals, social scientists, cyber experts, and information warriors to unpack all the complexity behind them.

They require intelligence agencies that would coordinate their efforts with the law enforcement and state administration in order to hunt down and neutralize emerging threats. The population needs to be involved in this in order to establish trust in the communities as, at times, people carry vital information that would prevent the attacks from occurring. The people are both a

vulnerable target and an important resource in hybrid warfare in countering adversaries. Hybrid warfare is often characterized by irregular tactics and unconventional methods of attack; however, conventional military strength is still essential. The question is why India continues investing so heavily in conventional forces if the probability of it facing a serious conventional war seems low. The reason is deterrence. Maintaining conventional deterrence ensures that India is not caught off-guard with hybrid threats that could escalate into full-blown conventional wars. By its very nature, hybrid warfare blurs the distinction between conventional and irregular combat. Lack of conventional readiness could leave India more vulnerable to even greater threats. Thus, conventional forces must be part of the broader strategy to counter hybrid warfare, but they must also be prepared to operate with specialized forces when dealing with non-conventional threats.

Hybrid warfare requires an integrated response, which goes beyond the military domain and embraces every aspect of national power. A "whole of government" approach is therefore crucial to achieving the effective countering of hybrid threats. This phrase essentially refers to the use of military, diplomatic, cyber, economic, and informational instruments in a coordinated manner. Military operations alone cannot help win hybrid warfare; they need to be supported through all spheres of government and society. Hybrid warfare strategies can only be efficiently executed at the highest levels of governance, bringing each tool of statecraft from military to non-military realms together in mutual support. So, for the Indian context, it would ensure military and civil agencies work very closely to realize all available capabilities for countering hybrid threats quickly and effectively.

One of the critical aspects of hybrid warfare is when and where to engage. Hybrid threats evolve over time, and the right tools must be applied at the right stage of the conflict. For instance, cyberattacks and information warfare may require a response from cyber agencies or law enforcement rather than military forces. Similarly, although in some instances military operations may be unavoidable, other hybrid tactics such as counter-radicalization or economic sanctions would require a non-military response (Gerasimov, 2013).

Hybrid warfare is not only fighting but also about understanding the wider context and socio-political dynamics that determine the conflict. India needs a comprehensive strategy to address the escalating threat of hybrid warfare. This strategy should include dialogue, analysis, and post-operation measures, incorporating both traditional and unconventional methods. Coordination between military and civilian systems is crucial for preventing, identifying, and eliminating threats.

Hybrid Warfare and Strategic Implications for India

The imprecise ambiguity in hybrid warfare, a complex issue involving military and non-military elements. India must respond swiftly to this hybrid threat scenario, ensuring regional security and national sovereignty. This hybrid warfare combines overt and covert actions, requiring nimbleness and subtlety.

Irregular armed groups and regular military forces blur the distinction between war and peace. It increased scale and speed and intensity of hybrid threats give rise to an increasing need for the strategy of security of countries. Being a country threatened both from outside as well as within India needs to know and counter hybrid warfare. Resilience is perhaps the most important thing in India's strategy in relation to hybrid warfare. Resilience through the inherent powers of the state, such as military strength and a strong networking intelligence system, besides strategic alliances can be properly used to deflect hybrid threats by India. The second, hybrid war does not correspond to conventional, irregular, or any other forms and categories of combat; it remains on a cline where any number of combinations of tactics is interwoven. Therefore, India's approach should be flexible, integrating diverse forms of combat and defence to address the full spectrum of threats.

Western Frontier: Hybrid War

The west border with Pakistan appears to be one of the most critical urgent areas, where hybrid warfare is likely for India. Such a strategy as used by Pakistan has been grossly accused more specifically in sponsoring terrorist organizations along with cross-border insurgencies along with cyberattack strategies. With this strategy coupled with sensitive territories such as in Jammu and Kashmir and in Punjab, results have been evident violence and uncertainty in the given areas. For instance, at Doda, Jammu and Kashmir, the loss of four lives reported recently have been encountered in the cross-border terrorism; thriving and on a high. Casualty figures over the last 32 months have been huge and underlines the constant risk hybrid warfare tactics present. The threats triggered a response from the Indian Army through extending its cooperation with the local law-enforcing agencies, to which the Jammu and Kashmir Police are also included, and designing a robustly inclined mechanism that will share the intelligence in countering the threats. Adding to the above is the increasing narco-terrorism across the border coupled with the use of drones for insurgent activities and that makes the security environment ever more complex. These are some, but only a part of the even broader hybrid strategy followed by Pakistan as advanced military capabilities converge in the direction with irregular tactics aimed to further destabilize India. All that is required from this aspect is continued building up India's collective defence capability while making preparation for this type of "war in shadows".

Hybrid Threats from China

A similar, yet even more complicated problem exists at the northern border of India. Three forms of warfare exist within the Chinese hybrid approach: psychological, political, and legal. These serve to manipulate perception, political process, and geopolitics. China has arguably applied its hybrid approach most masterfully through its United Front Work Department by employing front

organizations in attempts to shape opinion within the PRC as well as globally. For instance, another Chinese innovative hybrid tactics is that it increasingly depends on the commercial security operations outside of its borders and quasi-military forces in the maritime domain. Indirect intervention by China through this method threatens the security of the region, as it can be well noted in places like the Indian Ocean. With the increasing globalization of China, India needs to be prepared to meet not only the direct challenges but also the indirect challenges from an increasingly active neighbour in the North in hybrid operations (Jankowski, 2015).

Hybrid external threats are one part of a challenge for India; there is a formidable lot of internal insurgencies. Terror activities in Jammu and Kashmir, continuous unrest in Manipur, and continuous Naxalite insurgency along central India add further complexity into India's internal security scenario. And, thus, with terror attacks—actually, especially in places like Jammu and Kashmir as well as all other conflict places—showing an increasing upward trend, there is the presentation of the most diversified kinds of threats India may be facing in its variant of hybrid warfare. Narco-terrorism and the new dimension of drone infiltration from Pakistan into Punjab have caused Prime Minister Narendra Modi to take stock of the security situation to discuss and work upon counterterrorism efforts against it. This is a prudent call for a wholistic response.

Defence Strategy

The new and emerging threats require that India's defence strategy now must have hybrid warfare included in the broad security framework. The response mechanism needs to be integrated into India, which needs to include mechanisms by infusing conventional military capabilities with irregular tactics, cyber defence, and intelligence operations. While responding in an effective way, India needs to focus on national and regional resilience. It must strengthen the forces guarding the border and invest in technologies for deployment towards advanced and sophisticated warfare capabilities while arming the armed forces to counter hybrid tactics.

In this scenario, India would also have to be agile and nimble in defence strategy. One cannot afford a 'one-size-fits-all' approach for defence. Instead, it requires an agile defence framework that will enable the country to react against internal insurgencies and asymmetric warfare tactics just as much as against conventional threats posed by adversaries like Pakistan and China. The approach would be all-inclusive and integrated across the entire gamut of military, diplomatic, economic, and informational domains. Since hybrid threats are dynamic, there are several strategic moves by India that can help it adjust to this kind of threat and increase preparedness for it. One of them is that India needs to incorporate the tactics of hybrid warfare in its military doctrine, thereby incorporating hybrid strategies into the operational mandates of security forces. This approach will focus on enhancing coordination among the armed forces, intelligence agencies, and other security organizations to present

a more comprehensive and effective response to these threats. Information sharing and intelligence cooperation among relevant agencies should also be improved (Mockaitis, 1995).

Such effective communication and collaboration will transform the intelligence into actions that can then be executed quicker and with precision against hybrid threats. The Indian armed forces must make collaborative efforts toward executing joint exercises with strategic partners for better interoperability and cooperation. That would eventually add to the strength of being well-prepared against hybrid warfare. Third, India should worry about the hybrid threats it receives from its neighbours. China and Pakistan are not different in using their hybrid approach. It will help India understand the security structures and the threat that might come from these countries and thereby anticipate and pre-empt security challenges.

The second significant recommendation is the strengthening of strategic partnerships; India needs to take care of the enhancement of its partnership with Russia and other Eurasian states to solve hybrid threats, particularly in the Indian Ocean region, where influence from China is spreading very rapidly. In addition to conventional defence policies, India needs to focus more on soft power by strengthening qualitative research and developing alternative paradigms for foreign and security policy. This would help in lesser adversarial activities and make India more influential in international forums. Hybrid warfare is becoming an all-pervasive, multidimensional threat; thus, India needs to evolve its defence strategy to handle such challenges more effectively. A package approach that combines conventional military tactics with cyber defence, intelligence operations, and diplomatic efforts must form the crux of measures to enhance the resilience of India against hybrid threats. Only such an adaptive flexible strategy, which is both interaction with strategic allies and informed of intrinsic as well as extrinsic patterns, can build a much-needed basis to protect Indian national interests besides safeguarding stability at the region.

Conclusion

For India, the hybrid warfare scenario demanded a holistic, adaptive approach because conventional and unconventional threats come hand-in-hand as a package. And from the research conducted above, it becomes obvious that hybrid warfare is no longer an abstract; it is a grim reality that India has to face. This new interplay between conventional military force, irregular tactics, cyber warfare, disinformation campaigns, and economic coercion has completely changed the character of conflicts that require a shift in the defence strategy for India. For decades, hybrid warfare has been an operational reality for India's two major adversaries: Pakistan and China. The long-term strategy of Pakistan has been the launching of a state-sponsored terrorism and support insurgency across the border coupled with cross-border radicalization, thus posing an asymmetric threat to India on the western front. Economic pressure, cyber intrusions, legal manoeuvring, and information operations by China represent

a much more pervasive and sophisticated hybrid warfare model (Kofman, 2018). These pose a dual-front challenge to India, which would require a multidimensional response, in terms of preparedness of the military, cyber resilience, intelligence capabilities, and diplomatic agility.

Equally urgent is the inside-out version: Insurgencies in Jammu and Kashmir and the Naxalite movement point out weakness areas, if one were seeking vulnerabilities for probing. Hybrid warfare threats impact all areas—from social cohesion to economic stability—that may transcend simply from conflicts lines and into impact systems of governance at political dimensions, where higher penetrations of misinformation on social networks, the rise of narco-terrorists and the exploitation of any form of dependency, speaks to a war exceeding the conventional battleground confrontation. This complex, changing threat matrix demands that India shift from reactivity to proactivity in its security posture. Hybrid warfare strategy must focus on the four critical areas as follows: Hybrid warfare is an overarching term for the non-traditional tactics; a strong conventional force requires deterrence. India should upgrade her armed forces and integrate counter-insurgency, counter-terrorism, and cyber-defence capabilities. Special operations forces, psychological warfare units, and cyber command structures will enhance India's efficiency in carrying out hybrid warfare.

Cyber and Information Warfare Readiness: Hybrid conflicts will largely revolve around cyber warfare and information operations. India must, therefore, build a strong cyber defence mechanism that protects critical infrastructure from state-sponsored attacks. Disinformation and propaganda countering needs sophisticated narrative-building strategies with active engagement from state and independent media to influence public perception and combat enemy influence operations.

Intelligence and Early Warning Capabilities: Hybrid threats demand enhancement in intelligence capacities so that actions could be prevented and people may be alerted accordingly. In the case of hostile hybrid tactics, the requirement is for intelligence agencies to have a more extended framework of Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Open-Source Intelligence (OSINT). The issue also requires law enforcement agencies, intelligence services, and the military to work in conjunction with each other to tackle possible threats.

Whole Government and Whole Society Approach: Hybrid warfare not only targets military institutions but also forces the entire weakening of nations by vulnerabilities in the political, social, and economic spheres. An integrated approach from India will also include coordination with the government, engagement with the private sector, and civil society participation in order to building economic resilience, political stability, and societal cohesion towards countering hybrid threats.

Strategic Partnerships and Regional Alliances: India has to reach out to other such nations of similar ideas to share intelligence, develop collective capabilities of the armed forces, and help chart out joint security agreements with them as contours of hybrid warfare begin to emerge in international

relations. Strategic cooperation with the US, Russia, and QUAD (India, Japan, Australia, and the US) would do well to push back at the rising Chinese influence and asymmetric warfare in Pakistan.

Hybrid warfare constitutes the defining security challenge of the 21st century and hence requires a response that must be evolved and dynamic from the Indian perspective. The blurring of lines between war and peace, state and non-state actors, and conventional and unconventional threats underlines the necessity for India to increase its preparedness. This would translate to the finding, therefore, that India would require, in defence against hybrid threats, an element of multidimensional integration as a military modernization approach and through cyber defence, intelligence sharing, strategic partnerships, and societal resilience. An adaptive strategic approach involving a wide array of capabilities is key to success in hybrid warfare. India must review its national strategies, develop a 'whole of government' approach, and boost its military capabilities to tackle hybrid threats. This includes developing Intelligence, Surveillance, and Reconnaissance (ISR) capabilities, information warfare capabilities, and inducting new technologies into its warfighting capacities. India's strategic and political spaces must be integrated to effectively tackle hybrid warfare. It would thereby secure the sovereignty and territorial integrity of the nation, but also make India an important actor in the new security order that the world is set to become.

References

Ahluwalia, V. K., & Kapoor, R. (2019). Emerging challenges and the way ahead. In *Surprise, strategy and 'Vijay': 20 years of Kargil and beyond*, edited by V. K. Ahluwalia & N. Singh (pp. 39–45). Pentagon Press.

Aronsson, A. (2019). *The state of current counter-hybrid warfare policy*. Multinational Capability Development Campaign (MCDC). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf

Bjerregaard, T. (2012). *Hybrid warfare: A revolution in military affairs or an evolving threat*. Oxford University Press.

Caliskan, M. (2019). *Hybrid warfare and strategic theory*. Taylor & Francis.

Chellaney, B. (2017, August 27). China is waging a water war on India. *Hindustan Times*. https://www.hindustantimes.com/analysis/china-is-waging-a-water-war-on-india/story-6jqgabEffcatPFzJ6fQ6eJ.html

De Wijk, R. (2012). Hybrid Warfare. In *The Oxford Handbook of War*, edited by J. Baylis, J. Wirtz, & C. S. Gray Oxford University Press, 288–299.

Dheeraj, P. C. (2016, October 16). Evolving response to Pak's hybrid warfare. *Deccan Herald*. https://www.deccanherald.com/content/575629/evolving-response-paks-hybrid-warfare.html

Exum, A. (2006). *Hizballah at war: A military assessment*. Washington Institute for Near East Policy.

Gerasimov, V. (2013). *The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations*. Military-Industrial Courier (p. 112).

Gompert, D. C. (2007). *Heads we win: The cognitive side of counterinsurgency*. RAND Corporation.

Hoffman, F. G. (2006). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
Hoffman, F. G. (2007). Hybrid warfare and challenges for the future military force. *Joint Forces Quarterly*, *52*(1), 34–45.
Hoffman, F. G. (2010). *Complex irregular warfare: The next revolution in military affairs*. National Defence University Press.
Jankowski, M. (2015). Cyber warfare in hybrid conflicts: A case study of Russia's cyber operations in Ukraine. *Journal of Strategic Studies*, *38*(3), 25–39.
Johnson, D. (2019, March 30). *Review of speech by General Gerasimov on the vectors of the development of military strategy*. NATO Defense College. http://www.ndc.nato.int/research/research.php?icode=585
Kofman, M. (2018, March). *Hybrid warfare and Russian strategy*. Wilson Center.
Kumar, A. (2023). China's two-front conundrum: A perspective on the India–China border situation. *ORF Occasional Paper, (393)*. Observer Research Foundation.
Livermore, D. A. (2017). *Pakistan's support to the Taliban for strategic depth against India*. Carnegie Endowment for International Peace.
Mattis, J. N., & Hoffman, F. G. (2005). Future warfare: The rise of hybrid wars. *United States Naval Institute Proceedings Magazine*, *131*(11), 18–19.
Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. US Army War College Press.
Mockaitis, T. (1995). *Low-intensity operations and hybrid warfare*. Oxford University Press.
Niruthan, N. (2016, June 25). *How hybrid warfare could change Asia*. The Diplomat. https://thediplomat.com/2016/06/how-hybrid-warfare-could-change-asia/
Pandit, R. (2018, September 25). Unified tri-service agencies to handle cyberspace, space, special ops. *Times of India*. https://timesofindia.indiatimes.com/india/unified-tri-service-command-to-handle-cyberspace-space-special-operations/articleshow/65941584.cms
Sinha, U. K. (2016). *Riverine neighbourhood: Hydro-politics in South Asia*. Pentagon Press.
Sloan, E. (2017). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.
Smith, R. (2006). *The utility of force: The art of war in the modern world*. Knopf.
Tenenbaum, E. (2015). The evolution of hybrid warfare: Tactics and strategy in the 21st century. *Strategic Studies Quarterly*, *9*(4), 12–30.
Thornton, R. (2015). The changing nature of modern warfare: Russia, hybrid warfare, and the future of conflict. *The RUSI Journal*, *160*(4), 40–48.
Walker, R. G. (1995). *The hybrid threat: Understanding the future of conflict*. US Marine Corps Thesis.

16 Changing Dimensions of Hybrid Warfare

Emerging Threats to India in the 21st Century

Saddam Hussain

Introduction

Wars between states have occurred throughout the age of human civilization. Previously, they were conducted primarily to ensure interests, secure boundaries, capture natural resources, and spread the ideological understanding of preferred phenomena related to human life. This has resulted in wars during the periods of imperialism, colonialism, and World Wars I and II, followed by the Cold War and several destructive and coercive wars since that time. In our present-day technologically advanced society, human life and human security have been facing multidimensional conflicts that are non-kinetic, non-conventional, and irregular in nature. State-sponsored actors and non-state actors equipped with sophisticated and lethal tactics of warfare have emerged as a major threat to states in contemporary times. The synergy of this conventional to non-conventional, kinetic to non-kinetic, and regular to irregular warfare with the help of technology, cybernetics, artificial intelligence (AI), and robotics in military terminology is known as hybrid warfare. This study employs a descriptive-analytical research methodology to examine the definition, types, patterns, and evolving nature of hybrid warfare. The old traditional theory of hybrid warfare, which regarded it as largely 'an amalgamation of irregular warfare tactics with conventional mode of warfare in the battlefield', has been totally changed in the 21st century. Hybrid warfare has minimized the role of traditional physical warfare by stressing the greater importance of cognitive, technological, cyber, hacking, information, and data breaching, and other aspects of non-conventional warfare. The changing dimensions of hybrid warfare in contemporary times have produced alarming, yet unpredictable and unknown threats to states. Traditionally, the tools of hybridity in warfare tactics were used by the state-sponsored actors, and it was somehow traceable and defendable based on the capacity of the state in the given situation. In recent times, however, due to the man-machine interface, AI, cybernetics, data breaches, etc., and the proxy support of the state in operations by non-state actors has produced an entirely difficult and non-defendable (most of the time) threat to states. The very integration of the states and economic institutions in the globalized liberal economic system compelled nation-states to connect

DOI: 10.4324/9781003633204-19

through every available medium. The Internet and digital communication have become the backbone of the financial transactions of states, and any security lapse in them provides the hybrid terrorists with the very path to financial fraud. Not only this, but the Internet and digital platforms have become an accessible gateway to data theft, data breaches, data manipulation, and privacy protection in our everyday lives.

India, as one of the major players of South Asian geopolitics, has been targeted countlessly on hybrid grounds of warfare. As a multi-religious, multicultural, and ethnically diverse country, India has been particularly prone to hybrid warfare throughout its period of independence. India, in the 21st century, has mostly suffered from a three-layered hybrid warfare. The domestic insecurity, exploiting religious, casteist, linguistic, and ethnic sentiments, constitutes the first layer in the spectrum of a hybrid threat against India. The second layer is made up of the international pressure on India, using issues related to the country's internal politics, propaganda guided by particular flashpoints, the channelling diplomatic discomforts, and the protests of international actors and institutions. This has made continuous attempts to destabilize India's role in global politics. Finally, the infiltration, skirmishes, clashes, boundary alteration, propaganda, and digital threats from both China and Pakistan, respectively, constitute the third layer in the spectrum. Several reports have highlighted that communal unity and integrity in India are breached by financial support and brainwashing tools by adversary states/non-state actors. China and Pakistan have attacked India employing both conventional and hybrid warfare tactics to erode the path of the latter's leadership role in South Asian geopolitics. Some European states, and also the US, have been making use of our cultural diversity as a propaganda tool to reshape their global politics. Pakistan, through its propaganda-building mechanism, and China, through the manipulation of confidential information of economic and national importance, produced a multilayered hybrid threat to India. Hybrid warfare encompasses all the spheres of threat that possibly go against any state. Broadly, due to its complex nature, unpredictable anchors, and technocratic sophistication, it transcends all of India's security domains. The alarming threat of hybrid warfare has been identified and analyzed according to the defence and political setup in India. This chapter is divided into three sections: in the first section of the chapter attempts have been made to provide a conceptual understanding of hybrid warfare and its connotations; the second section of the chapter provides an insight of the different dimensions of the hybrid warfare; and the final section of the chapter delineates with the hybrid threats to India, in the three-layered spectrum of hybrid security. The section also attempted to describe, in very brief terms, the counter-strategy mechanism the New Delhi administration has taken in the domain of hybrid warfare. It was very difficult for the author to address all the dimensions of hybrid threat in one single chapter; thus, an attempt has been made to describe the common dimensions and domains of hybrid threat in brief.

Conceptualizing the Term

Hybrid Warfare has been a contested concept among military strategists and historians for a considerable time. Broadly, this term refers to a 'process of military strategy blended with conventional and non-conventional, regular-irregular, kinetic-non-kinetic, and digital methods of war'. Frank Hoffman has described hybrid threats as incorporating a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict. The effects can be gained at all levels of war (Hoffman, 2007). The term used to illustrate Hezbollah's warfare tactics against Israel in summer 2006 has received special attention from the Russo-Crimean war of 2014, which included non-conventional warfare methods in order to gain strategic leverage. Hybrid Warfare, in its current outlook, was popularized by the speech of Admiral James Mattis of the US Marine Corps at the Defence Forum backed by the Marine Corps Association in 2005 (Frank, 2005). Later on, Lieutenant Colonel of the US Marine Corps Frank Hoffman theorized hybrid warfare as a military strategy of conventional warfare blended with non-conventional warfare strategies such as irregular, political, and cyber-warfare using fake news, propaganda, diplomacy, and lawfare (Wither, 2016). In another contribution, military historian Peter Mansoor has defined hybrid warfare as conflict involving a combination of conventional military forces and irregulars– guerrillas, insurgents, and terrorists, including both state and non-state actors, aimed at achieving a common political purpose (Mansoor, 2012). Although these definitions are new in origin, the idea of irregular tactics of warfare is nothing new. Many centuries ago, for example, India's traditional realist thinker and military adviser Kautilya advised the Swami (King) on the importance of Sama (Conciliation), Dama (Economic gratification), Danda (Use of force), and Bheda (dissension) as warfare strategies. As early as the 5th century BC, Chinese philosopher Sun Tzu advised that in all battles the direct method ensures the joining of forces in battle, but the indirect method is the one that ensures victory. The German-Austrian military historian von Clausewitz stated that war is a policy by other means, and hence, that hybrid warfare is a warfare tactic with 'other' methods. These classic examples are enough to believe in hybrid warfare as an age-old concept.

In contrast to the traditional hybrid methods of war deception, propaganda, treaty, assimilation, proxy warfare, etc., hybrid wars in the contemporary world is more ambiguous. It not only effectively leverages available technologies, but also strategically exploits religious, economic, and cultural sentiments of the masses, thereby shaping hybrid warfare into a more complex and multifaceted form. This kind of popular support of a large common mass

has been reflected in Hezbollah's war against Israel, the War on Terror strategy, the Taliban's War against America in Afghanistan, and Vietnam's guerrilla war against America. Hezbollah's war against Israel, staged in summer 2006, reflects a complex and alternative structure of warfare in comparison with the Western model of militia (Hoffman, 2007). The group's guerrillas stood their ground with their hi-tech weaponry and guerrilla tactics. They operated in a decentralized manner at tactical levels, from both their urban and their mountain bases, and shocked the Israeli Defence Forces (IDF) with their conventional-cum-unconventional forms of warfare (Ahluwalia, 2019). The major contribution to Hezbollah, a Shia militia group of Lebanon, has come from Iran, and it comes in the form of religious assistance to the guerrilla warriors of Hezbollah. The support from Iran's Shia community and the tactical use of Lebanese domestic outrage against Israel certainly provide this small non-state actor with a major victory in the hybrid war against the powerful Israel (Ahluwalia, 2019). Similar results have been reflected in America's War on Terror strategy against the Taliban. After a lengthy, twenty-year tussle, NATO forces were compelled to leave Afghanistan. The case of the withdrawal of the army by leaving the people in turmoil under the Taliban in 2022 has been criticized by the native Americans and concerned intellectuals throughout the globe. Before the withdrawal of the forces from Afghanistan, America's intervention, the deployment of the army, and human rights violations in Afghanistan in the name of the War against Terror were also criticized by a major section of society. The activities in the case of Hezbollah's strategy against Israel have been described as 'Perception Dominance', in David Betz's *The Idea of Hybridity*, by which he meant "An act of not just dominating one's foe physically but undermining them morally and psychologically, tunnelling out their base of support domestically as well as their reputation internationally" (Betz, 2019). Strategic analyst Sean Monaghan has opined that "Hybrid wars use multi-domain warfighting approaches, including cyberattacks, disinformation and subversion, economic blackmail and sabotage, sponsorship of proxy forces, and creeping military expansionism to destabilize a society or a nation by influencing its decision-making process without resorting to traditional conflict" (Monaghan, 2018). These are some important literary works on the subject, and as there is no universally accepted definition of hybrid warfare, there is an ambiguity existing among scholars on the subject. However, the common consensus is that hybrid warfare is a war by other means, an uncertain war, an unpredictable war, a 'grey zone' warfare skill sometimes referred to as fifth-generation warfare. It has been one of the most difficult warfare tactics since ancient times, but the technological integration of warfare skills has turned it into perhaps the most lethal warfare tactic.

The intricate nature of contemporary hybrid warfare lies in its pervasive, everyday character, leaving states often uncertain about the nature of the attacks, the identities of the aggressors, and the underlying motives behind these actions. These asymmetric threats pose serious questions for the defence systems of states in contemporary times. Though most of the studies on the

subject emphasized the importance of non-military tactics, it is not the case that these operations are always conducted by non-state actors. In her analysis, Margaret Bond, for example, emphasized the "employment of comprehensive and highly nuanced varieties of military activities, resources, programs, and applications…" (Bond, 2019). Her study stressed that hybrid threats are not aired on the web; rather, they are an inevitable threat to the emerging security structure in India. The recent reports of military personnel in India echo these hybrid threats in strong words. A state's vulnerability to a hybrid threat lies in the fact that it is possible at both the inter-state and intra-state levels. This chapter goes on to analyse the possible threat structure resulting from the changing dimensions of hybrid warfare in India in contemporary times.

Energy Security, AI, and the Evolving Landscape of Hybrid Warfare

An analytical review of the recorded history of humanity shows that violence and conflict are central themes which have shaped world politics. Contemporary warfare poses significant challenges for military strategists, especially with an escalation in the Hybrid Warfare strategy, which greatly complicates the landscape. Hybrid warfare strategy primarily aims to undermine a state's economic development and, consequently, its energy security and stability. The relationship between hybrid warfare and control over energy resources is crucial in international relations. Russia, the US, Israel, Iran etc. have strategically leveraged this connection for over a decade, integrating it into their military and geopolitical strategies. Russia's annexation of Crimea in 2014 illustrated the effectiveness of employing "deniable" special forces, local armed groups, economic leverage, disinformation, and the strategic manipulation of socio-political divisions in Ukraine to achieve its goals. An equally important, yet often underappreciated aspect of this episode was Russia's decisive disruption and blockage of energy supplies. Before the annexation, Crimea was almost entirely reliant on mainland Ukraine for its energy needs. To solidify its political control, Russia promptly nationalized the Ukrainian company *Chornomornaftogaz*, along with all its onshore and offshore energy assets. This pre-emptive action ensured Russia's uninterrupted energy transport to the annexed territory, effectively exploiting Crimea's dependency on Ukrainian energy resources (Rühle, 2015). Energy security is an absolute essential; it guarantees the reliable availability of energy sources at affordable prices, forming the backbone of national stability. Both a robust infrastructure and diverse supply chains are imperative to ensure uninterrupted energy flow, which is vital for both economic strength and military readiness.

The link between energy security and hybrid warfare is clear and compelling. Dominating energy resources provides a significant strategic advantage in conflicts, as adversaries will tend to exploit energy supply disruptions as tactical weapons. Nations that depend excessively on single energy sources expose themselves to serious vulnerabilities. Therefore, diversification and bold investment in renewable energy are not just options—they are essential for fortifying

national resilience. While reliance on energy resources poses certain vulnerabilities, states can decisively counter these risks through strategic diversification and strong national security frameworks. Hybrid warfare and energy security are both vital components of national security, each serving distinct and critical functions. Hybrid warfare disrupts by targeting both military and civilian sectors, enabling objectives to be met without resorting to full-scale conflict. In contrast, energy security is fundamental to ensuring a stable, reliable, and affordable energy supply. This goal is achieved through the robust protection of supply chains, the strategic diversification of energy sources, and decisive investments in infrastructure. This chapter will provide an in-depth examination of the evolving dynamics of hybrid warfare and their critical implications for India's national security strategy in the 21st century. By recognizing these two distinct dimensions of national security, it becomes imperative to explore their interplay in a separate and dedicated study.

The evolving landscapes of hybrid warfare have become increasingly complex by introducing the man–machine interface with the help of cybernetics, AI technology, weapons of mass destruction, bio-engineering, usage of biological and chemical weapons, and information and data available on social sites. The integration of robotics, unmanned vehicles, and advanced machine training has enhanced the dimensional framework, introducing critical variables that redefine system modeling and performance assessments. AI stands as a revolutionary technological advancement that has decisively established itself in the 21st century, driven by swift innovations and an abundance of data crucial for any state or society. It is crucial to understand that AI does not have any direct historical connection to the strategic principles of warfare. While hybrid warfare effectively leverages AI technologies—such as drones and data analytics for intelligence gathering—the essence of hybrid warfare resides in its strategic methodology, rather than in the specific technologies employed. Its primary purpose is to significantly enhance both efficiency and effectiveness, making it an indispensable asset in any form of conflict. AI actively contributes to numerous facets of hybrid warfare, from refining information warfare techniques to elevating decision-making processes. However, the tactics and strategies of hybrid warfare stand independently of AI. The distinction between the two is unmistakable—hybrid warfare is a methodology of engagement, whereas AI encompasses a wide range of technologies that enable these engagements. Therefore, hybrid warfare and AI are distinct concepts, each playing focused, yet complementary roles. In summary, hybrid warfare provides a powerful strategic framework for the grasping of modern conflicts, while AI functions as a formidable technological tool that underpins various military operations. While a definitive consensus remains elusive, scholars in warfare studies largely concur that hybrid warfare and grey zone conflict represent distinct yet interconnected paradigms. These concepts are frequently employed interchangeably to characterize the ambiguous and uncertain maneuvers of states in international politics. However, there is a basic distinction. Grey zone warfare is solely dedicated to ambiguous, uncertain, and below-threshold moves of a

state, while hybrid warfare covers a much wider canvas of irregular, uncertain, ambiguous, and skilful use of force by state or non-state actors to destabilize the peace and stability of a state, to halt the economic growth of a state, or to pursue other, wider objectives. It accommodates the methods which were not present in pre-industrial warfare. These ultra-modern hybrid methods have appeared as important tools of offence and defence. The ability to achieve a 'first strike' has surprisingly increased with this kinetic medium of attack.

Hybrid warfare is a longstanding concept that is well-recognized by the global community. The very aim of hybrid warfare is not only to undermine the opponent's military might but also to bring about the infrastructural destruction, societal disintegration, and economic breakdown of the adversary through the usage of cyber-attacks, ransomware, the misuse of social networking sites, online fraud, etc.

Throughout history, influential military strategists and political thinkers such as Kautilya, Thucydides, Sun Tzu, and Machiavelli have all underscored the significance of hybrid strategies. On the battlefield, iconic military leaders such as Alexander the Great, Genghis Khan, Napoleon, Babur, and Shivaji have all successfully employed these strategies to seize power. Furthermore, British and other imperialist forces have effectively harnessed hybrid tactics to conquer formidable nations. The dynamics of the Cold War serve as a striking illustration, showcasing Soviet Union–American cooperation as a prime example of non-conventional warfare. However, until the end of the Cold War, the realm of hybrid or irregular warfare remained largely confined to fixed battlefields and predictable patterns. Today, by contrast, we are witnessing a substantial shift like the growth of traditional hybrid warfare in the post-Cold War environment. The crucial role of hybrid warfare in the changing dimensions is that it expands the war zone from a conventional battlefield to a more blurred and unpredictable grey zone. The actors of hybrid warfare are no longer limited to state-sponsored militaries; rather, it is carried out by non-state actors and even by people with ideological differences. The economic liberalization and unilateral dominance of the United States have undeniably sparked valuable discussions and challenges in unconventional ways. The terrorist attacks on September 11, 2001, marked a pivotal turning point, clearly demonstrating the formidable capabilities of non-state actors such as Al-Qaeda in opposing superpower influence. This event raised urgent questions about the effectiveness of security intelligence strategists in our contemporary landscape and mandated a thorough reassessment of national security policies. Since the 9/11 attacks, non-state actors have expertly navigated the complexities of the battlefield, effectively engaging with major powers in various dimensions. Groups such as the Taliban, Hezbollah, and Houthi guerrillas, along with numerous terrorist organizations, have adeptly utilized the Internet, digital communication platforms, and social networking sites to assert their influence and execute their tactics of warfare. Recognizing these dynamics empowers us to cultivate a more assertive dialogue around security, strategy, and global cooperation in tackling the challenges posed by non-state actors.

Major Hybrid Threats to India in the 21st Century

India has appeared as one of the major players in contemporary geopolitics. The rising profile of the country in global politics inevitably brings forward asymmetric threats within and beyond territorial boundaries. The possibility of the asymmetric threat of hybrid warfare to India's global interests is an inevitable reality. Since its creation, Pakistan has been using non-conventional methods of hybrid warfare against India through the ideological radicalization of Kashmiris. India has responded with a conventional deterrence strategy against this threat; in recent times, however, these Kashmiri separationists have been upgraded with hybrid skills. These militants have been assigned with the task of creating 'fearful silence in the valley' which is detrimental to economic integration and social developments in Kashmir. Officials report that these operations were undertaken by 'part-time militants' at the direction of Pakistan's spy agency ISI, and they do it in a much more organized way (Desk T. H., 2021). The "dismemberment remarks" of Pakistan's president in 1971,"We will bleed India by a thousand of cuts," shows the evil for adopting any warfare methods to hurt India, politically, economically, socially, militarily, and irregularly, through the use of techniques such as propaganda and information warfare. Since, then and precisely in the 1980s, proxy war has been a common method for Pakistan to destabilize India's national security. In the period following the war between the Soviet Union and Afghanistan, Pakistan has made sophisticated use of Afghan jihadi troops against India. The Jihadi terrorists were trained in guerrilla techniques of irregular warfare and they jeopardized the security structures in Kashmir for decades. The brainwashing of talented youths of Kashmir on different social and ideological grounds has also been used as an irregular warfare technique by the ISI. With intense support from China, Pakistan appeared as a more tangible threat to India's global power aspirations. This has been reflected in China's move in the UN Security Council on the abrogation of Article 370 in the Indian Constitution on Kashmir's special provision (Roy, 2020). However, India loudly condemned this move by China, stressing it to be an internal matter: "India does not comment on the internal affairs of other countries and similarly expects other countries to do likewise." This was a statement made by a spokesperson from the country's Ministry of External Affairs, India.

The cyber domain of the hybrid threat makes it more complex as it breaches the very nerve of economic progress through cyber fraud; since 2004, 14.9 billion accounts have been leaked, and about 254.9 million of these are users from India. It has been found that India's breach rate was 740% higher than the first quarter, as of June 1, 2022, rising from 5 to 42 breached accounts in a minute cyber security company Surf-shark said in its report (Tan, 2022). During the period of June to July 2022, around 2,000 websites were successfully hacked by 'Dragon-force Malaysia' and 'Hacktivist Indonesia.' The Cyber Police in Ahmedabad reported these incidents to government of India and Interpol for the actions of these groups, which included the scanning, breaching, and

blocking of sensitive websites operating in India (Sikarwar, 2022). A report by CERT-IN, India's cyber watchdog, claimed that in 2022, India experienced a 51% increase in cyber-attacks compared to 2021, across all sectors, from healthcare services to power supply. In a digitally advanced society, the preservation of online information and data is essential to the secure delivery of consumer services. The databases involved online trading/networking and government sites hold information that is highly sensitive in nature. A data breach may pose a serious threat to public life, and government agencies may be rendered non-functional in terms of discharging services based on digital platforms. Why are cyber data breaches so impactful? The answer to this question is reflected in some classical examples. For instance, WikiLeaks founder Julian Assange, through his release of about 4900 confidential documents, revealed much of the brutal behaviour of US forces in the Iraq and Afghanistan Wars in the name of global security (Times, 2022). There is a separate matter of academic discussion as to whether or not what Assange had done was wrong. In this case, however, the absolute failure of US intelligence has been witnessed by the strategic community throughout the world. This data breach has called into question the dignity and credibility of the US in global politics. The next case of a data breach is also related to the same country. In this case, Hamza Bendelladj, a 27-year-old Algerian computer engineer, who used a Trojan Horse piece of banking software called SpyEye to steal millions of dollars, which he donated to Palestinian charity organizations. Again, this chapter is not going to make a judgement about what Hamza did. The point is that it questioned the credibility of US security intelligence. The crucial impact of this has been analysed by US Attorney Sally Quillian Yates, in the following terms: "In a cyber-netherworld, he allegedly commercialised the wholesale theft of financial and personal information through this virus, which he sold to other cyber-criminals" (Hatuqa, 2015). This is an advanced pattern of strategic information warfare using cyberspace, microcomputers, and associated information technologies (Molander, 1996). These incidents are displaying the alarming threat of data leaks based on confidential information in the cyber age. India, the world's most populous state, and one with a low literacy rate, is particularly prone to cyber-attacks, and on numerous occasions has been targeted by cyber terrorists. According to a report by IBM titled 'Cost of a Data Breach 2022', the average cost incurred by an organization due to a data breach is approximately US$4.35 million. It was also stated that about 83% of companies have experienced more than one incident of data breach (Krishnan, 2023). There have been a number of such scandals: In an Air India data breach case, the personal information of 4.5 million persons was stolen; similarly, the personally identifiable data and the test results of the 1,90,000 Common Admission Test(CAT)applicants were obtained by hackers who put them on sale on a cybercrime forum (the CAT is a national test for management studies conducted by the Indian Institute of Management); the security systems of Upstox, India's second-biggest stock broking firm in terms of clients, were breached in April 2021 by hackers who obtained KYC (Know Your Customer—A service

used in India to map the authenticity of customers in digital and financial communications) and other associated information of 25 lakh customers. According to a Times of India report (2022), the data theft was traced to a third-party warehouse, and the documents were uploaded on the dark web (Krishnan, 2023). One of India's most prominent civil nuclear facility centres, Kudankulam, has also been targeted by cyber terrorists. In this case the Ministry of State for Atomic Energy and Space Jitendra Singh attempted to reassure people by remarking that the cyber-attack had occurred in the administrative block, and not in the plant. The cyberattacks assume importance given the increased state of hostilities in the Indian subcontinent (Bhaskar, 2019).

The fundamental architecture of the internet creates significant obstacles in effectively countering or deterring malicious cyber operations from foreign entities. Rapid and accurate attribution of disinformation campaigns, ransomware deployments, or data breaches is highly complex. This complexity often makes it challenging to identify the responsible actors promptly and with high confidence. Nevertheless, recognizing these challenges is crucial for developing robust strategies to enhance our cybersecurity resilience.(Mallick, 2023). In contemporary certitude, critical hybrid challenge to India came from China. China, given its close relationship with Pakistan, has utilized and instrumentalized its asymmetric war against India. China considers India not only a geopolitical competitor but also a strategic threat to its hegemonic leadership. The hybrid threats from China to India are more potent, complex, crucial, lethal, and dynamic. The most crucial challenges come in the domain of cyber security. China has been spying on India's confidential data through its surveillance tools. In August 2022, China docked its spy ship *Yuan Wang 5* (designed for satellite and missile tracking and operated by the People's Liberation Army Strategic Support Force) at Sri Lanka's Hambantota port. This raised serious concerns in India about its surveillance capabilities (Tan, 2022). Similarly, the development of Nepal's Lumbini Airport, geographically proximate to the Indian border, creates a tangible security threat to New Delhi. The Belt and Road Initiative (BRI), the China–Pakistan Economic Corridor (CPEC), and the associated infrastructural advancements within India's periphery have significantly heightened the geopolitical tensions among strategic analysts in New Delhi. These initiatives are not merely aimed at enhancing financial investments in the participating countries; they are also crafted to ensure access to critical strategic intelligence that directly influences India's national security and regional stability (Singh, 2022).

In addition to the espionage, China has consistently targeted India through the deployment of AI technology and cyber capabilities. Numerous Chinese applications have been specifically engineered to gather critical data concerning public life and governmental operations within India. A significant number of these applications have functioned without securing requisite approvals from regulatory authorities and have evaded compliance with tax obligations mandated for digital enterprises. It highlights the dual threat of financial fraud and critical data breaches. The subsequent ban of some Chinese mobile apps is

the result of the actions New Delhi has taken in recent years. During his visit to New Delhi, Google's vice president, engineering, privacy and security revealed that India had witnessed 18 million cyber-attacks in the first quarter of 2022, reaching a height of about 200,000 in a single day. In the same visit, he highlighted that about 30% of transactions in India were digital, the highest percentage in the world; however, the flip side is that the same technology may be used for financial fraud (Sur, 2022). The latest data breach reported by IBM and Ponemon in 2021 highlighted a cumulative loss of $4.24 million throughout the world. An investigation conducted by Indian Express revealed that more than 10,000 organizations and persons are being monitored, tracked, and kept under surveillance by a leading tech company with links with the Chinese Communist Party. The Shenzhen-based tech firm, Zhenhua Data Information Technology Co. Ltd., has been accused of for tracking the president of India, the prime minister, cabinet ministers, serving and ex-chiefs of the Indian armed forces, chief ministers, the chief justice, comptroller and auditor general (CAG), bureaucrats, scientists, academicians, journalists, industrialists, actors etc., in India (Chaudhury, 2022). India's defence, economic, communication, and public infrastructure, etc., are soft targets for adversaries in its hybrid war against India. The Indian government reported to parliament that between June 2018 and March 2022, the majority of the cyber-attacks were registered against private banks, in which hackers stole around 6861 crores along with business and personal information (Paul, 2022). State and non-state adversaries are increasingly employing robotics and artificial intelligence technologies to undermine India's ascendant power. This exploitation of advanced tech, particularly through the strategic manipulation of social media platforms like Facebook, WhatsApp, and YouTube, poses a significant threat in the realm of hybrid warfare. Hybrid warfare, often characterized by external provocation, seeks to capitalize on ethnic, religious, socio-economic, and cultural discord to destabilize and dismantle political regimes. The sophisticated misuse of these platforms serves to further erode communal harmony, thereby deepening societal divides and complicating India's political landscape. There exists a range of organized groups and institutions that function as provocateurs, aiming to incite communal violence and confrontations with authorities. They utilize both print and visual media, as well as manipulated videos and misinformation on social media platforms, to achieve their goals. Addressing these unique forms of violence poses significant challenges for military forces, as conventional strategies and machinery alone are insufficient. A robust response necessitates the active collaboration of a diverse coalition of experts, including those from foreign policy, political leadership, top-tier scientific researchers, computer engineers, media scholars, and distinguished professionals across science, humanities, and commerce (Bajhwa, 2020).

External support and supervision through social networking sites have threatened India's internal security structure. Radicalization of the youth by hybrid terrorists in order to recruit them to agencies like Lashkar e Taiba (LeT), Jaish e Mohammad (JeM), Islamic State of Iraq and Syria (ISIS), Al-Qa'ida in

the Indian Subcontinent (AQIS), etc. using Telegram and other social media sites challenged the strategic community at New Delhi. These youths are being constantly brainwashed by cybercrime planners across the globe through virtual sessions to spread propaganda and misinformation relating to sensitive issues among Indian youths. Some institutions operating in India are being financed by foreign countries to terrorize the social life and communal harmony in India. In a report by the Economic Times, it was revealed that in 2017 social media triggered seven communal clashes in a single month in the West Bengal province of India (Das, 2017). The extremism around the borders of the North-East, Kashmir, Nepal, and Bhutan is generating and spreading through state actors. India's neighbouring states, in particular, China, Pakistan, Bangladesh, and Myanmar, have been actively involved in breaching India's internal security structure, and the most appealing methods to spread turmoil among the internal security structure in India are detected in the 'guided misuse' of social media for pre-planned actions.

India needs to pay constructive attention to the emerging hybrid threats. It is an unpredictable, peculiar, and complex peacetime conflict and hence very difficult to detect. The strategic community in New Delhi has come to realize the importance of this subject and has started to take a serious interest to this alarming threat. In recent times, this has been reflected in the statements of Indian military veterans. India's first Chief of Defence Staff (CDS), Major General Bipin Rawat expressed the opinion that

> Future conflicts will be more violent and unpredictable with battlefields being severely contested and seamlessly connected. In the future, even conventional conflicts are likely to have profound elements of hybrid war. Technology has become a key driver of future wars.
>
> (Bureau, 2019)

Hybrid warfare could be employed against this multi-religious and multi-ethnic state in a hundred ways. Hence, India needs a strong counter-attacking strategy and mechanism aimed at protecting the country from hybrid threats in changing scenarios. The need for 'below threshold operations' has been reflected in an assessment study of Indian military planners. The study underscores a significant deficiency in updated military strategies across both kinetic and non-kinetic security domains. It highlights the integration of various interagency services in assessing military personnel capabilities. The capacity to conduct Cyber Network Operations (CNO) as a mechanism for addressing hybrid threats, an essential capability for modern armed forces, is clearly articulated within the current military strategy framework. In comparison to China, the Indian armed forces exhibit a limited degree of autonomy in conducting cyber operations. Consequently, India's Defence Cyber Agency is now advocating for a level of operational autonomy akin to that of China's Strategic Support Force (PLASSF) in the cyber domain.(Rathor, 2020). A change at the structural and operational level in the counter-terror strategy of the military

domain is essential at this time. This has resulted in a recent speech about the security environment in India's neighbourhood, in which the Air Chief Marshal talked about hybrid warfare. In this he emphasized capacity building for future warfare, which should be waged with cyber and information as tools of contemporary battle (Desk T.O.I, 2022). The need to build exclusive hybrid warfare tactics in all domains, political, economic, cyber, sea, space, land, and information warfare, has been echoed in recent speeches, reports, and workshops on military strategy.

In addition to military enhancement, the political and diplomatic methods should also be taken into account by the government. The strong will to protect the privacy and crucial information of its citizens and institutions should be ensured by the government. In peacetime, the government should come up with a mechanism that compels neighbouring states to think about the political solution to problems they have on boundaries or in intra-state affairs. In the domain of domestic security, any kind of extremism, be it the radicalization of minority youth or right-wing extremism, will require smart handling. Armed forces should be free from political pressure to launch immediate operations. The government should come up with strategies to curb the spread of violence, communal riots, and data breaches strongly and in an impartial manner. It is essential to achieve confidence building at the community level by providing each the space to negotiate on issues they felt necessary for their development and politics.

Summary

Building on the core assumption that the international system is anarchic, questions arise about how states, as the most important actors, seek to secure the ultimate prize they seek: security. The answer is twofold; states primarily use either coercion, or the prospect of coercion to attain their goals, and they do so through the application of strategy (Najzer, 2020). The nature of old-age irregular warfare has changed into a complex model of warfare with the fusion of technological improvements in contemporary times. Traditionally, India has been a nation with a conventional military strategy. In the changing dimensions of hybrid warfare, with the increased use of cybernetics, robotics, and information crucial to national security, the nature of the hybrid threat is likely to become more lethal and complex. The misuse of social media in India on numerous grounds has breached internal security mechanisms and there are reports that in these cases the direction to spread violence has been received from foreign lands waging a hybrid war against India. The espionage of sensitive and critical data through cyber-attacks represents a significant present-day economic and security threat to India. Therefore, it is imperative to implement a robust counter-strategy that integrates both kinetic and non-kinetic approaches, encompassing conventional and non-conventional tactics. This strategy must also leverage regular and irregular operations, along with collaborative defence mechanisms. India faces a critical gap in political will and the infrastructural

capacity necessary for effective counter-operations and a credible 'first-strike' capability. Military planners must take decisive action to identify, investigate, and develop advanced strategies and technologies in order to confront this sophisticated form of warfare. Moreover, this study outlines a proactive counter-terrorism strategy targeting institutions within the country that aim to destabilize and hinder progress. This research is poised to significantly enhance our understanding of the evolving dimensions of hybrid warfare and will serve as a vital resource for those engaged in this field. Additionally, this chapter calls on strategic thinkers and students to delve into the multifaceted aspects of hybrid warfare as a distinct discipline, emphasizing the urgent need for targeted research that reflects the dynamic nature (AI, energy, information warfare, software and hybrid warfare etc.,) of the most unpredictable and ambiguous conflict.

References

Ahluwalia, L. G. (2019). Hybrid Warfare: Battlegrounds of the Future. *Center for Land Warfare Studies*, Vol. 12, No. 2, pp. 15–34.

Bajhwa, L. G. (2020, February 10). *India under a Hybrid Attack?!* Retrieved September26, 2022, from indiandefencereview: http://www.indiandefencereview.com/news/india-under-a-hybrid-attack/

Betz, D. (2019). The Idea of Hybridity. In *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, edited by V. K. Fridman (pp. 9–25). London: Lynne Rienner.

Bhaskar, U. (2019, November 20). *India Confirms Malware Attack at Kudankulam Nuclear Power Plant*. Retrieved from livemint.com: https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html

Bond, M., cited in P.K. Chakravorty (2019), Hybrid Warfare in the Sino-Indian context. *Centre for Land and Warfare Studies (CLAWS)*, Vol. 12, No. 2, pp. 80–95.

Bureau, W. (2019, July 13). *Future Conflicts Will Be More Violent, Unpredictable, Says Army Chief General Bipin Rawat*. Retrieved September27, 2022, from outlookindia: https://www.outlookindia.com/website/story/india-news-future-conflicts-will-be-more-violent-unpredictable-says-army-chief-general-bipin-rawat/334120

Chaudhury, D. R. (2022, June 5). *CCP-Linked Chinese Companies Kept the Personal Data of Indians*. Retrieved September25, 2022, from The Economic Times: https://economictimes.indiatimes.com/news/india/ccp-linked-chinese-companies-kept-personal-data-of-indians/articleshow/92012600.cms?from=mdr

Das, M. (2017, July 8). *Social Media Posts Trigger Seven Communal Riots in a Month in West Bengal*. Retrieved September27, 2022, from The Economic Times: https://economictimes.indiatimes.com/news/politics-and-nation/social-media-posts-trigger-seven-communal-riots-in-a-month-in-west-bengal/articleshow/59496771.cms?from=mdr

Financial Express (2022, June 14). *Data Leaks: India Is Sixth on the Global Breach List, and this CERT-IN Directive May Worsen the Situation*. Retrieved September23, 2022, from Financial Express: https://www.financialexpress.com/life/technology-india-data-security-personal-data-leaks-surfshark-cert-in-2560424/

Frank, M. N. (2005, November 2). *Future Warfare: The Rise of Hybrid Wars*. Retrieved on September22, 2022, from https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars:https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

Global Times (2022, June 20). *Assange Case Mirrors Hypocrisy of UK and US in Protection of Press Freedom: Chinese FM*. Retrieved September24, 2022, from Global Times: https://www.globaltimes.cn/page/202206/1268564.shtml

Hatuqa, D. (2015, September 15). *Hamza Bendelladj: Is the Algerian Hacker a Hero?* Retrieved September25, 2022, from Aljazeera: https://www.aljazeera.com/news/2015/9/21/hamza-bendelladj-is-the-algerian-hacker-a-hero

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

Krishnan, A. (2023, May 9). *Top 7 Data Breach Incidents in India*. Retrieved from ET Edge: Insights: https://etinsights.et-edge.com/top-7-data-breach-incidents-in-india/

Mallick, P. K. (2023). Information Warfare: Time for a Relook. In *Indian Armed Forces in 2047 at the Centenary of Independence*, edited by L. G. Banerjee (pp. 185–204). New Delhi: Pentagon Press LLP.

Mansoor, W. M. (2012). *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to Present*. Cambridge: Cambridge University Press.

Molander, R. C. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica: RAND Corporation.

Monaghan, S. (2018). *Countering Hybrid Warfare So What for the Future Joint Force? Features*, 82–98. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf

Najzer, B. (2020). *The Hybrid Age: International Security in the Era of Hybrid Warfare*. New York: I. B. Tauris.

Paul, M. (2022, August 4). *Data Protection Bill: India Stood 2nd in Data Breaches in Jan-Jun 2022*. Retrieved September26, 2022, from https://www.livemint.com/industry/telecom/data-protection-bill-india-stood-2nd-in-data-breaches-in-jan-jun-2022-11659607001742.html

Rathor, M. S. (2020, December). Hybrid Warfare Challenges to Indian Defence Forces. *Centre for Land Warfare Studies Journal*, Issue Brief No.260, 1–10.

Roy, S. (2020, August 6). *China Raises J&K issue at Security Council*. Retrieved September23, 2022, from Indian Express: https://indianexpress.com/article/india/china-raises-jk-issue-at-security-council-6541447/

Rühle, M. (2015). Energy as a Tool of Hybrid Warfare. *NATO-Research Paper*, *113*, 1–8.

Sikarwar, D. (2022, August 12). *The Growing Cyber Threat to India from Far East*. Retrieved September23, 2022, from The Economic Times: https://economictimes.indiatimes.com/news/india/imf-warns-inflation-may-stay-high-sees-need-for-monetary-tightening/articleshow/101883366.cms

Singh, B. K. (2022, August 18). *Spies, Lies, and China's Invisible War against India*. Retrieved September25, 2022, from moneycontrol: https://www.moneycontrol.com/news/opinion/spies-lies-and-chinas-invisible-war-against-india-9050771.html

Sur, A. (2022, August 25). *India Saw 18 Million Cyber Attacks in First Quarter of 2022: Google's Royal Hansen*. Retrieved September25, 2022, from moneycontrol: https://www.moneycontrol.com/news/business/india-saw-18-million-cyber-attacks-in-first-quarter-of-2022-google-executive-royal-hansen-9084911.html

Tan, Y. (2022). Chinese "spy ship" Yuan Wang 5 docks in Sri Lanka despite Indian concern, retrived on September 30, 2022 from https://www.bbc.com/news/world-asia-62558767

The Hindu (2021, July 5). *'Hybrid' Militants, a New Challenge for Security Forces in Kashmir*. Retrieved September23, 2022, from The Hindu: https://www.thehindu.com/news/national/other-states/hybrid-militants-a-new-challenge-for-security-forces-in-kashmir/article35139620.ece

Times of India (2022, September 20). *Security Environment in Neighbourhood Far from Ideal, Must Prepare for Hybrid Warfare*. Retrieved September27, 2022, from Times of India: https://timesofindia.indiatimes.com/india/security-environment-in-neighbourhood-far-from-ideal-must-prepare-for-hybrid-warfare-iaf-chief/articleshow/94327083.cms

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*, Vol. 15, No. 2, pp. 73–87.

Index

Pages in *italics* refer to figures, pages in **bold** refer to tables, and pages followed by n refer to notes.