

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES

POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

EDITOR
Tuhina Sinha

**GLOBAL CRISES AND SYSTEMIC
VULNERABILITIES: POLITICAL ECONOMY OF
CLIMATE CHANGE AND DIGITAL SECURITY-
2026**

**ISBN: 978-625-93102-0-6
DOI: 10.5281/zenodo.18281748**

**Edited By
Tuhina Sinha**

January / 2026
İstanbul, Türkiye



Copyright © Haliç Yayınevi

Date: 17.01.2025

Halic Publishing House

İstanbul, Türkiye

www.halicyayinevi.com

All rights reserved no part of this book may be reproduced in any form, by photocopying or by any electronic or mechanical means, including information storage or retrieval systems, without permission in writing from both the copyright owner and the publisher of this book.

© Halic Publishers 2025

The Member of International Association of Publishers

The digital PDF version of this title is available Open Access and distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 license (<http://creativecommons.org/licenses/by-nc/4.0/>) which permits adaptation, alteration, reproduction and distribution for noncommercial use, without further permission provided the original work is attributed. The derivative works do not need to be licensed on the same terms.

adopted by ESRA KOÇAK

ISBN: 978-625-93102-0-6

Copyright © 2025 by Haliç Academic Publishers All rights reserved

**GLOBAL CRISES AND SYSTEMIC VULNERABILITIES:
POLITICAL ECONOMY OF CLIMATE CHANGE AND
DIGITAL SECURITY**

EDITOR

Tuhina Sinha

AUTHORS

Dr. Dharmendra Jayantilal AMBANI

Dr. Santoshi MISRA

Dr. Sirisha DAVID

Jatinkumar Bhimjibhai KOTADIYA

Hetal Pravinsinh JADEJA

Huzaifa AHMAD

TABLE OF CONTENTS

PREFACE.....	i
CHAPTER 1	
CYBERSECURITY AND DIGITAL VULNERABILITIES IN	
TIMES OF POLITICAL AND ECONOMIC CRISIS	
Jatinkumar Bhimjibhai KOTADIYA	
Dr. Dharmendra Jayantilal AMBANI	
Hetal Pravinsinh JADEJA	1
CHAPTER 2	
CLIMATE CHANGE AS AN ECONOMIC AND POLITICAL	
CRISIS	
Huzaifa AHMAD	31
CHAPTER 3	
CLIMATE CHANGE AS A GLOBAL, POLITICAL-	
ECONOMIC CRISIS: MATHEMATICAL MODELLING AND	
POLICY PERSPECTIVES	
Dr. Santoshi MISRA	
Dr. Sirisha DAVID	52

PREFACE

Global crises today are no longer confined to a single field or region; they spread rapidly across economies, societies, and political systems. Climate change, digital insecurity, and systemic vulnerabilities have become deeply interconnected challenges that shape the future of governance, development, and human security.

This book, “Global Crises and Systemic Vulnerabilities: Political Economy of Climate Change and Digital Security,” brings together diverse academic perspectives to examine how political and economic dynamics influence both environmental threats and emerging digital risks. By combining theoretical discussions with policy-oriented approaches, the chapters aim to provide a clearer understanding of these multidimensional crises and their long-term consequences.

We hope this volume will serve as a valuable resource for researchers, policymakers, and readers interested in global political economy, climate governance, and cybersecurity debates.

Editorial Team

January 17, 2025

Türkiye

CHAPTER 1
CYBERSECURITY AND DIGITAL
VULNERABILITIES IN TIMES OF POLITICAL AND
ECONOMIC CRISIS

Jatinkumar Bhimjibhai KOTADIYA¹

Dr. Dharmendra Jayantilal AMBANI²

Hetal Pravinsinh JADEJA³

¹Department of Computer Science, Atmiya University, Rajkot, India, jatin.kotadiya123@gmail.com, ORCID ID: 0009-0004-4643-2690

²Department of Computer Science, Harivandana College, Rajkot, India, dharmendraambani@gmail.com, ORCID ID: 0009-0006-5126-4331

³Department of Computer Science, Harivandana College, Rajkot, India, hetal.hvc@gmail.com, ORCID ID: 0009-0008-4429-3489

INTRODUCTION

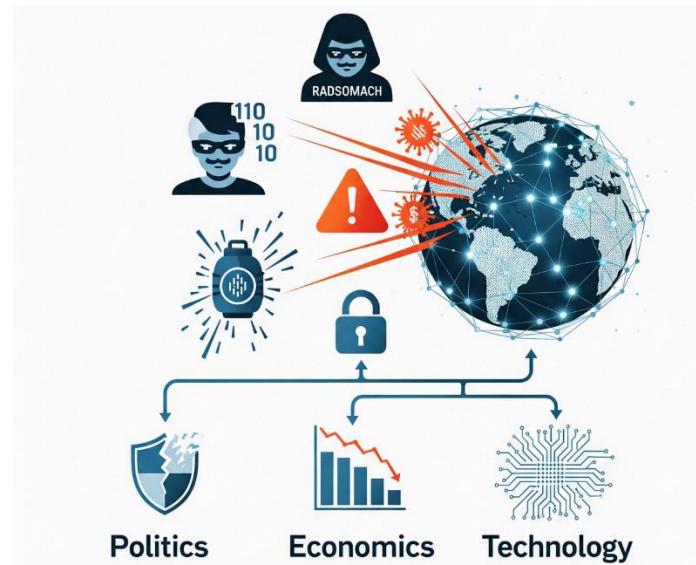


Figure 1. The Global Digital System: Intersections of Politics, Economics, and Technology

The growing integration of digital technologies into political and economic systems has reshaped the global landscape of international political economy (IPE). As states, markets, and societies increasingly rely on interconnected digital infrastructures, the potential risks associated with cyber threats have expanded considerably. Cybersecurity is no longer a technical or sector-specific issue; it has become a structural concern that influences questions of sovereignty, economic stability, power distribution, and governance (Baldoni & Di Luna, 2025; Stepan & Trushkina, 2025).

Disruptions in financial networks, supply chains, and critical infrastructure have revealed that vulnerabilities in cyberspace can intensify political and economic crises, transforming local issues into worldwide instabilities (World Economic Forum, 2022; IBM Institute for Business Value, 2024). In the context of IPE, cybersecurity is located at the intersection of politics, economics, and technology, influencing the strength of developed and emerging economies as they confront increasing digital dependencies (OECD, 2025; Tuteja, 2025).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The significance of studying digital vulnerabilities becomes particularly pronounced during times of political and economic crisis. Financial problems, fights between countries, and health crises are getting worse because of cyber-attacks that make people lose faith in organisations, weaken market confidence, and intensify existing divisions between states and societies (Maurer, 2021; Natalucci et al., 2024). Ransomware attacks on essential services, cyber-enabled disinformation campaigns, and coordinated assaults on infrastructure illustrate how digital vulnerabilities function as crisis multipliers rather than isolated threats (Cyberly, 2024; RUSI, 2024). Furthermore, the digital divide leaves emerging economies disproportionately exposed, while advanced economies face escalating risks tied to complex supply chains and critical technological dependencies (World Economic Forum [WEF], 2025; Baldoni & Di Luna, 2025). By analysing these vulnerabilities within the broader context of international political economy (IPE), it becomes possible to understand how cyber threats not only destabilise governance but also reconfigure the distribution of power and influence across the global system.

This chapter aims to explore the intersection of cybersecurity and digital vulnerabilities in times of political and economic crisis, situating these dynamics within the theoretical and practical frameworks of IPE. The primary objectives are threefold: first, to conceptualize cybersecurity as a structural element of the global political economy; Second, look at how cyber attacks affect crises in areas like finance, energy, healthcare, and defense; and third, check what this means for how governments and countries work together and stay stable. To achieve these objectives, the chapter seeks to address several guiding research questions: How does cybersecurity shape the resilience of political and economic systems during crises? In what ways do digital vulnerabilities exacerbate existing instabilities across global markets and governance structures? What roles do state and non-state actors play in both mitigating and exploiting cyber risks in crisis contexts? And finally, how can international cooperation and policy frameworks evolve to address these emerging challenges effectively?

The chapter is organized into several key sections. Following this introduction, the next section defines cybersecurity within the framework of IPE and elaborates on its political, economic, and theoretical dimensions.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Subsequent sections explore the ways in which cyber incidents intensify crises across critical sectors, supported by case studies such as ransomware attacks, the Colonial Pipeline incident, and cyber operations linked to geopolitical conflicts. Attention is also directed toward global supply chain vulnerabilities, the persistence of the digital divide, and the heightened risks faced by emerging economies. The chapter then examines the role of various actors including governments, international organizations, private corporations, and malicious groups in shaping the cybersecurity landscape. Further analysis considers governance challenges and the absence of universally binding norms. The last part talks about possible future dangers from new technologies like artificial intelligence, blockchain, Web3, and quantum computing. It then suggests ways to make systems stronger, encourage teamwork between government and businesses, and help growing areas develop their abilities. By following this structure, the chapter provides a comprehensive examination of cybersecurity as a defining factor in understanding political and economic crises in the digital age.

1. CONCEPTUAL AND THEORETICAL FOUNDATIONS

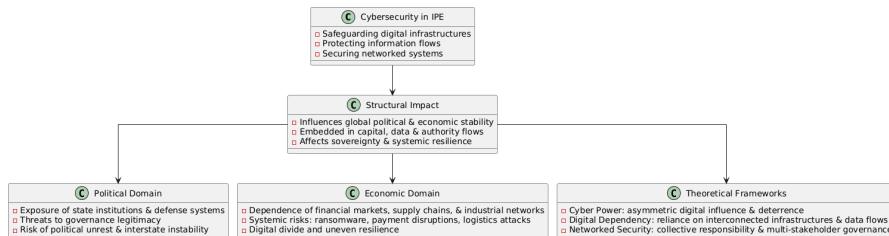


Figure 2. Cybersecurity in International Political Economy (IPE) – Conceptual & Theoretical Foundations

Within the discipline of International Political Economy (IPE), cybersecurity can no longer be understood as a narrowly technical or purely national security concern. Instead, it must be recognized as a structural issue that influences global political and economic stability. Cybersecurity here means protecting digital systems, the flow of information, and connected networks that support activities like trade, finance, government operations, and security.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

From an IPE viewpoint, cyber risks are part of how money, information, and power move across countries, so they can't be separated from how countries rely on each other and the way the world order works. Financial institutions, international supply chains, and essential systems are becoming more reliant on global digital platforms. This means that weaknesses in these platforms can have wide-reaching effects, go beyond individual countries and shaping the balance of power between nations. So, looking at cybersecurity through the idea of IPE makes scholars and policymakers think about digital threats in the bigger picture of national control, how systems can withstand problems, and how international relationships are changing.

Digital vulnerabilities operate simultaneously in political and economic domains, magnifying instability during times of crisis. Politically, the vulnerability of state institutions, electoral systems, and defense frameworks to cyberattacks weakens the legitimacy of governance and endangers the stability of international relations (Andini et al., 2023; BAE Systems, 2024). Intrusions that disrupt government communication or hinder essential services can erode public confidence, provoke political unrest, and escalate existing conflicts (Romavella, 2024; Paulis, 2025). Economically, the reliance of financial markets, industrial systems, and supply chains on digital frameworks generates significant systemic risks (World Economic Forum [WEF], 2025; Konecka & Bentyn, 2024).

Incidents such as ransomware attacks, breakdowns of payment systems, or strikes on logistics platforms underscore the considerable effect of digital reliance on global economic stability (Accenture, 2025; McKinsey & Institute of International Finance, 2024). Moreover, the ongoing digital divide results in unequal resilience: advanced nations usually invest in more robust defensive measures, while emerging markets are more vulnerable to disruptive impacts, thereby exacerbating existing disparities (WEF, 2025; World Bank, 2024). When integrated, these factors suggest that digital vulnerabilities are not merely technical issues but deep-rooted flaws that interact with political and economic crises, often intensifying their severity.

To better understand these dynamics, researchers have utilized theoretical frameworks including cyber power, digital dependency, and networked security.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The notion of cyber power highlights how both states and non-state actors deploy digital capabilities to project influence, deter adversaries, or destabilize rivals. Unlike traditional forms of military or economic power, cyber power operates asymmetrically, enabling smaller or weaker actors to challenge stronger ones with disruptive digital tools. The concept of digital dependency sheds light on the reliance of economies and governments on interconnected infrastructures, cloud ecosystems, and transnational data flows that are often controlled by a small set of global corporations or technologically advanced states. Such dependency generates new vulnerabilities that can be strategically exploited in times of crisis, raising urgent questions about autonomy and sovereignty. Meanwhile, the framework of networked security underscores the collective nature of cybersecurity challenges. Because digital infrastructures are globally interconnected, no state can secure itself in isolation. Cybersecurity should be seen as a problem where everyone is connected and needs to work together. It requires all parties—governments, international groups, and businesses to take responsibility, cooperate, and engage with each other to address the challenge effectively. These ideas together show how cybersecurity works as both a tool for power and a weakness in the global economy, affecting how authority, trust, and the ability to bounce back are spread in a world that's becoming more digital.

2. CYBERSECURITY IN POLITICAL AND ECONOMIC CRISES

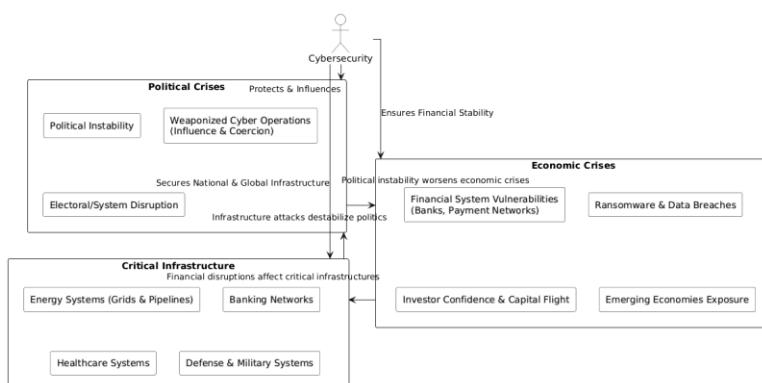


Figure 3. Cybersecurity in Political and Economic Crises

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The interconnection between cybersecurity and crises in the international political economy has become increasingly apparent in the twenty-first century. Political instability, economic downturns, and systemic disruptions are now often accompanied, and sometimes intensified, by cyber incidents that exploit vulnerabilities in digital infrastructures. Cybersecurity is not simply a technical safeguard; it is a structural component of global resilience that directly shapes the outcomes of political conflicts, economic turbulence, and institutional stability. As the world economy becomes more reliant on digital systems, not dealing with cybersecurity risks could make problems worse, mess up how governments work, and make people lose faith in political and economic institutions. Cybersecurity also plays a decisive role in global political conflicts by functioning both as a protective shield and as a weaponized tool of influence. When combined, these dynamics indicate that digital vulnerabilities are not just technical failures but foundational flaws that engage with political and economic crises, frequently exacerbating their intensity (Beyer, 2023; Maurer, 2022).

These actions blur distinctions between traditional warfare and information warfare, making conventional notions of sovereignty and security more complex (Chatham House, 2019; Maurer, 2022). For example, cyber activities aimed at electoral systems, government databases, or media outlets can disrupt local political processes, diminish public trust, and change the nature of international discussions (Canadian Centre for Cyber Security, 2024; Kennan Institute / Harvard Kennedy School, 2018). Consequently, cybersecurity has evolved from a minor concern to a vital component of geopolitical strategy, underscoring that digital weaknesses are now intertwined with political power conflicts (OSTI, 2025). The role of cybersecurity becomes increasingly important during financial crises, as vulnerabilities in global economic systems are already more pronounced. Modern financial institutions depend heavily on digital platforms for transactions, clearing, and settlement, creating multiple points of exposure that attackers can exploit (Maurer & Nelson, 2021). Cybercriminals and state-sponsored groups frequently take advantage of such moments of instability to launch large-scale data breaches, ransomware assaults on banks, or manipulations of financial information systems (BigID, 2024; Maurer & Nelson, 2021).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The disruption of payment networks or theft of digital assets undermines investor confidence, accelerates capital flight, and worsens economic distress in fragile markets (IMF, 2024). The increasing integration of emerging economies into global financial networks has expanded the digital attack surface, leaving weaker regulatory systems more exposed to systemic shocks (Adrian & Ferreira, 2023; Kalash, 2025). In this context, cybersecurity emerges as a vital determinant of financial resilience, shaping how effectively economies can recover and maintain stability in times of fiscal turbulence.

The threats extend further to critical infrastructures, which form the backbone of national and international stability. Energy systems, such as electricity grids and oil pipelines, are especially attractive targets because disruptions can paralyze economies and destabilize international supply chains. Banking networks, too, are frequent subjects of sophisticated attacks intended to undermine financial stability and public trust. In the healthcare sector, cyber incidents pose unique risks by disabling hospital systems, delaying treatments, or exposing sensitive patient data—vulnerabilities that became especially visible during global health emergencies.

Defense infrastructures are equally at risk, as cyber intrusions may target command systems, weapons technologies, and logistical networks, thereby weakening national security. The interdependence of these infrastructures means that a successful cyberattack on one sector often cascades into others, magnifying the impact of crises across entire economies and regions. Strengthening the cybersecurity of critical infrastructures is therefore essential not only for national security but also for sustaining the stability of the global political economy during times of volatility.

3. DIGITAL VULNERABILITIES IN THE GLOBAL ECONOMY

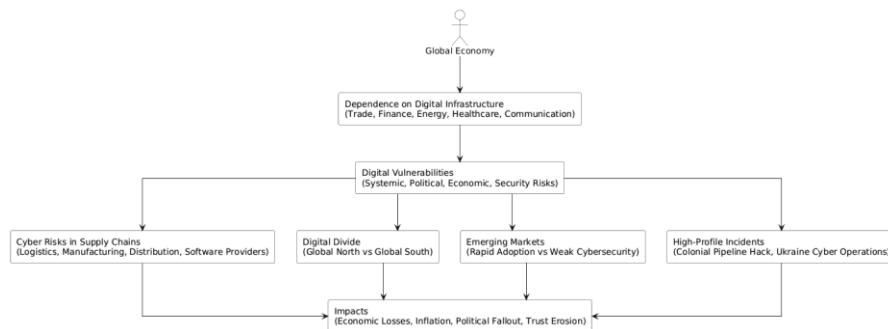


Figure 4. Digital Vulnerabilities in the Global Economy

The global economy has become increasingly dependent on digital infrastructures that underpin trade, finance, energy, healthcare, and communication systems. While these advancements have facilitated efficiency, connectivity, and innovation, they have also exposed states and markets to unprecedented forms of risk. Digital vulnerabilities today extend beyond isolated technological failures; they intersect with political instability, economic crises, and security threats, amplifying systemic fragility. In this context, cyber risks in global supply chains have emerged as one of the most pressing challenges.

The digitization of procurement, manufacturing, and distribution processes has created multiple points of entry for cyberattacks. A single disruption—such as the compromise of a logistics management system or ransomware targeting shipping operators—can paralyze the movement of goods across borders. Attacks on software providers and suppliers have cascading effects that ripple through entire networks, magnifying economic losses and weakening state capacities to respond effectively. In highly interdependent economies, supply chain cyberattacks can exacerbate inflationary pressures, destabilize trade relations, and undermine trust in international markets, demonstrating that cybersecurity has become a critical determinant of supply chain resilience in the global economy.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Another layer of vulnerability stems from the persistence of the digital divide between industrialised nations in the Global North and developing states in the Global South. Advanced economies often benefit from well-funded cyber-defence institutions, private-sector innovation, and strong regulatory environments. By contrast, many developing economies remain constrained by limited resources, weak institutional capacity, and inadequate technical expertise (Kshetri, 2016; Timcke, Gaffley & Rens, 2023). This asymmetry not only heightens vulnerabilities in the South but also introduces risks for global interdependence, as cyber threats originating in less secure regions can propagate across borders (World Economic Forum [WEF], 2025; Rajagopalan, 2023). Unequal resilience undermines collective security efforts and risks reinforcing patterns of dependency and exclusion within the international political economy (Heeks, 2021; Parikkar, 2024). Addressing this divide is therefore not simply a matter of development but also a prerequisite for global economic stability and shared digital security (WEF, 2024; Calderaro & Craig, 2020).

Emerging markets occupy a particularly precarious position within this dynamic. On the one hand, their rapid adoption of digital technologies drives economic growth, financial inclusion, and participation in global commerce (World Economic Forum, 2023). On the other hand, this accelerated integration often outpaces the establishment of robust cybersecurity frameworks. These markets typically rely on imported technologies, outsourced digital services, and foreign capital, making them susceptible to both external manipulation and internal exploitation (Delphos Cybersecurity, 2025). Financial systems in such economies are increasingly targeted by cybercriminals who exploit weak defenses in banking and payment infrastructures (World Bank, 2023). Moreover, political institutions in emerging markets are frequently the subject of disinformation campaigns and election-related cyber operations, threatening both democratic legitimacy and investor confidence (Lemos, 2024). Such vulnerabilities create conditions where a single cyber incident can disproportionately destabilize national economies and erode social trust (AInvest, 2025). Several high-profile incidents illustrate the disruptive capacity of these digital vulnerabilities in times of political and economic crisis.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Ransomware attacks, which have proliferated globally, highlight the financial and operational costs of cyber insecurity. The Colonial Pipeline hack in 2021, which disrupted fuel supplies across the eastern United States, demonstrated how cyber incidents can trigger economic panic, supply shortages, and political fallout. Similarly, cyber operations linked to the Ukraine conflict underscore the use of digital warfare as a strategic tool, targeting both critical infrastructure and civilian networks to amplify instability. These cases confirm that cyberattacks are not confined to technical disruptions; they constitute structural threats capable of reshaping economic dynamics, eroding state legitimacy, and escalating geopolitical tensions.

4. STATE AND NON-STATE ACTORS IN CYBERSECURITY

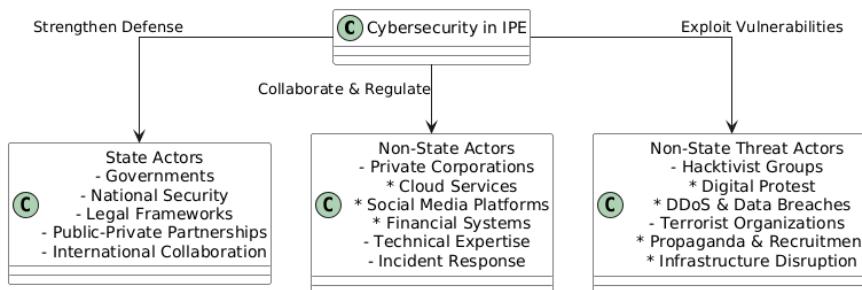


Figure 5. State and Non-State Actors in Cybersecurity

The dynamics of cybersecurity in international political economy are shaped by the interaction of both state and non-state actors, whose roles can either strengthen defenses or exploit vulnerabilities depending on their motivations and capacities. Governments occupy a central position in this ecosystem as they are responsible for protecting national security, safeguarding economic stability, and maintaining the integrity of critical infrastructure. Through the development of national cybersecurity strategies, legal frameworks, and specialized agencies, states attempt to establish strong defensive capabilities.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Many governments have also begun to institutionalize public-private partnerships and cross-border collaboration to counter cyber threats, while simultaneously engaging in international dialogues on cyber norms and governance.

Despite these efforts, the lack of universally binding agreements continues to undermine collective action, leaving cyberspace vulnerable to exploitation. Cybersecurity also plays an increasingly strategic role in geopolitics, with cyber warfare and espionage emerging as essential tools of modern statecraft. State-sponsored cyber operations, ranging from election interference and disinformation campaigns to the sabotage of energy and communication systems, reveal how digital tools can destabilize political systems and exacerbate economic crises (Hendin, 2020; Jindal, 2023; S&P Global, 2025). These activities often occur in the grey zone of international conflict, where attribution is contested and escalation risks remain high (Jindal, 2023; Iyengar, & Lukasik, 2024). The integration of cyber operations into national security strategies demonstrates how states view the digital domain as a space for projecting power and safeguarding sovereignty, making cybersecurity a central element in contemporary geopolitical rivalries (Odebade & Benkhelifa, 2023; Jindal, 2023).

Alongside governments, private-sector actors particularly large technology corporations—hold critical responsibilities in securing digital economies. Much of the world's digital infrastructure, including cloud services, social media platforms, and financial systems, is owned and managed by private enterprises. These companies often possess greater technical expertise and resources than many state agencies, positioning them as indispensable partners in cyber defense (United Nations Capital Development Fund [UNCDF], 2024; OECD, 2019). Their ability to detect, mitigate, and recover from large-scale incidents has made them vital stakeholders in the digital security landscape (International Telecommunication Union [ITU], 2024). However, their influence also raises concerns about accountability, transparency, and the alignment of corporate interests with broader public-policy objectives (World Economic Forum, 2019).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

As a result, cooperation between states and corporations is both necessary and challenging—requiring new forms of governance to address trust, jurisdiction, and regulatory gaps (OECD, 2019; OpenGov Asia, 2023).

Non-state actors such as hacktivist groups and terrorist organizations further complicate the cybersecurity landscape by exploiting vulnerabilities for ideological or disruptive purposes. Hacktivists often engage in digital protests against governments or corporations, using tools such as distributed denial-of-service attacks or data breaches to expose corruption or advance social causes. While sometimes framed as forms of digital civil disobedience, these actions can destabilize economies and erode public trust in institutions, especially during times of crisis. Terrorist organizations, on the other hand, increasingly use cyberspace for propaganda, recruitment, financing, and even attempts to disrupt critical infrastructure. The accessibility and anonymity of the digital environment grant such actors asymmetric advantages, making them difficult to monitor and counter effectively. Their activities underscore the democratization of cyber capabilities, where even small groups can generate significant disruption on a global scale. Taken together, the roles of state and non-state actors illustrate the complexity of cybersecurity in the international political economy. Governments, private corporations, hacktivists, and terrorist groups all contribute to shaping the digital landscape, either by reinforcing its resilience or by exploiting its vulnerabilities. In times of political and economic crisis, these interactions become even more consequential, determining whether cyberspace functions as a stabilizing force or as a multiplier of instability.

5. INSTITUTIONAL AND GLOBAL GOVERNANCE PERSPECTIVES

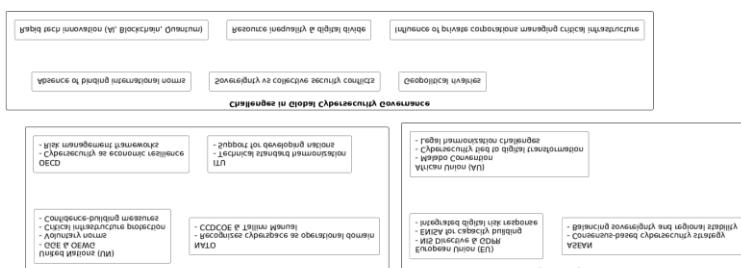


Figure 6. Global and Regional Cybersecurity Governance

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

International organizations have become central to the development of cyber norms and cooperative frameworks that regulate behavior in the digital domain. The United Nations (UN), through its Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), has been instrumental in promoting voluntary norms of responsible state conduct, focusing on the protection of critical infrastructure, the prevention of attacks on essential civilian systems, and the cultivation of confidence-building measures among states. NATO, by contrast, has adopted a more security-oriented approach, officially recognizing cyberspace as an operational domain alongside land, air, sea, and space.

Its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn has further advanced legal and strategic debates, particularly through the Tallinn Manual, which provides authoritative interpretations of how international law applies to cyber conflict. The Organization for Economic Co-operation and Development (OECD) has contributed by framing cybersecurity as a fundamental component of economic resilience, urging risk management frameworks and coordinated policies among its members. Likewise, the International Telecommunication Union (ITU) has emphasized harmonization of technical standards and global cooperation, with a strong focus on assisting developing nations in building their cybersecurity capacities. Despite these contributions, the diversity of priorities across institutions—ranging from security to development and economic stability—illustrates the fragmented nature of global cyber governance.

Regional organisations also reflect varied approaches to cybersecurity governance shaped by their political and economic contexts. The European Union (EU) has emerged as a leader in normative regulation, implementing instruments such as the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR). These measures emphasise not only resilience against cyber incidents but also the protection of individual rights in the digital domain (European Commission, n.d.; ENISA, n.d.). Complementing these legal frameworks, the European Union Agency for Cybersecurity (ENISA) supports Member States in capacity building and facilitates information-sharing, creating an integrated response to digital risks (ENISA, n.d.).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

In Southeast Asia, the Association of Southeast Asian Nations (ASEAN) has followed a more incremental, consensus-based strategy, balancing sovereignty concerns with collective security needs. Its Cybersecurity Cooperation Strategy underscores a pragmatic approach to fostering regional stability while accommodating diverse national priorities (ASEAN, 2022). The African Union (AU), in contrast, has linked cybersecurity directly to its broader goals of digital transformation and socio-economic development. The Malabo Convention on Cyber Security and Personal Data Protection represents a significant milestone in harmonising legal standards across African states, although difficulties in ratification and implementation persist (African Union, 2014/2023). Together, these regional approaches highlight the extent to which cybersecurity governance is influenced by institutional capacities, levels of integration, and regional political dynamics.

Despite these initiatives, establishing a cohesive and universally accepted system of global cybersecurity governance remains elusive. One of the principal challenges lies in the absence of binding international norms: while many states endorse voluntary principles, diverging national interests prevent the adoption of enforceable rules. The conflict between sovereignty and collective security complicates efforts to build consensus, as states remain reluctant to relinquish control over their digital infrastructure. Geopolitical rivalries intensify this fragmentation, with major powers often treating cyber negotiations as extensions of strategic competition. Furthermore, the rapid pace of technological innovation—including developments in artificial intelligence, blockchain, and quantum computing—outstrips the capacity of regulatory frameworks to adapt, leaving governance mechanisms perpetually behind technological realities. The uneven distribution of resources between developed and developing nations deepens the digital divide, making it difficult for less-resourced states to comply with or benefit from emerging cyber norms. In addition, the growing influence of private corporations in managing critical digital infrastructure complicates governance, as these actors operate transnationally and wield power that often rivals that of sovereign states. Taken together, these factors underscore the urgent need for adaptive, inclusive, and multi-stakeholder approaches that can effectively address the global nature of cybersecurity challenges.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Such approaches must acknowledge the interconnectedness of digital vulnerabilities and the shared responsibility of states, international organizations, and private actors in safeguarding cyberspace during times of political and economic crisis.

6. CYBERSECURITY AS A POLITICAL AND ECONOMIC CRISIS MULTIPLIER

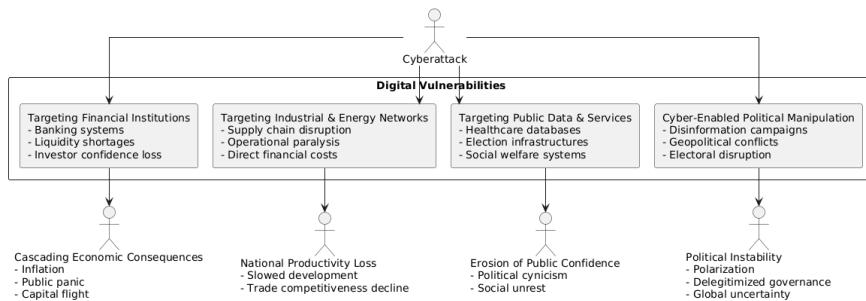


Figure 7. Cybersecurity as a Political and Economic Crisis Multiplier

The accelerating reliance on digital infrastructures has elevated cybersecurity from a technical issue to a structural determinant of political and economic stability. Far from being isolated incidents, cyberattacks often intersect with existing vulnerabilities in national economies, governance frameworks, and international relations. In this sense, cybersecurity can act as a multiplier of crises, amplifying disruptions that originate in political or economic domains and transforming them into systemic threats.

Cyberattacks destabilize national economies by targeting financial institutions, industrial supply chains, and critical infrastructures. When banking systems are compromised, they risk triggering liquidity shortages, disrupting payment mechanisms, and undermining investor confidence. Similarly, breaches of industrial networks or energy grids not only impose direct financial costs but also paralyze sectors essential for national productivity. The Colonial Pipeline ransomware attack in 2021 vividly demonstrated how cyber intrusions can generate cascading economic consequences, including fuel shortages, inflationary pressures, and public panic.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

For emerging markets, where cybersecurity frameworks are often underdeveloped, the economic consequences of such incidents are even more severe, leading to capital flight, weakened trade competitiveness, and slower development trajectories.

Beyond direct economic effects, cyber incidents erode public confidence by exposing the inability of governments and corporations to safeguard sensitive data and protect essential services. Trust in state and economic institutions is central to maintaining political order and ensuring the smooth functioning of markets, yet large-scale breaches of healthcare databases, election infrastructures, or social welfare systems not only endanger individual privacy but also raise broader questions about institutional competence and legitimacy (Shandler, Gross, & Canetti, 2023; Gomez & Shandler, 2022). When citizens perceive that their governments are incapable of securing digital assets, political cynicism intensifies, and social unrest becomes more likely (Gomez & Shandler, 2022; Shandler et al., 2023). The erosion of public trust can also reverberate globally, as international investors and allies reconsider their commitments to states perceived as cyber-vulnerable (Natalucci, Qureshi, & Suntheim, 2024).

Digital vulnerabilities also act as powerful drivers of political instability by intensifying existing tensions and creating opportunities for exploitation by both state and non-state actors. Cyber-enabled disinformation campaigns, for example, have been instrumental in polarizing electorates and weakening democratic institutions. Similarly, cyber operations linked to geopolitical rivalries, such as those observed during the Ukraine conflict, illustrate how digital aggression can exacerbate territorial disputes and destabilize fragile political systems. In authoritarian regimes, digital vulnerabilities may embolden opposition groups or external actors seeking to undermine ruling authorities, while in democracies, persistent cyber disruptions can delegitimize electoral processes and contribute to populist backlashes. In both contexts, cybersecurity challenges magnify grievances, disrupt governance processes, and generate uncertainty in global economic and security alliances.

7. FUTURE CHALLENGES AND EMERGING TRENDS

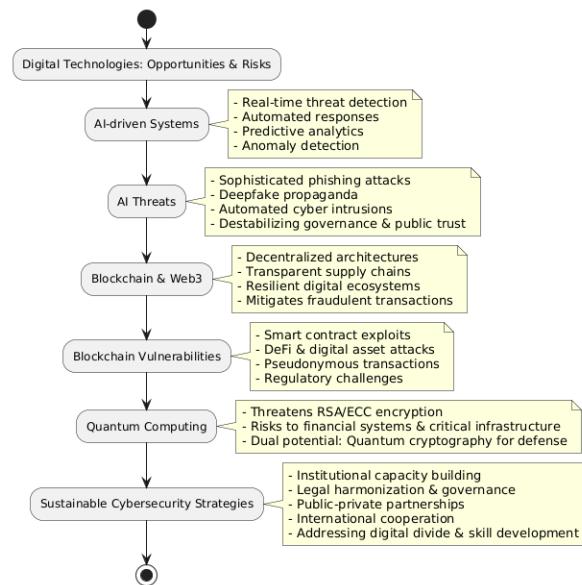


Figure 8. Future Challenges and Emerging Trends in Cybersecurity

The future trajectory of cybersecurity within international political economy is shaped by the rapid advancement of digital technologies that simultaneously create transformative opportunities and unprecedented risks. As political and economic systems become increasingly dependent on digital infrastructures, vulnerabilities in cyberspace evolve in scope, scale, and sophistication.

Artificial intelligence (AI) exemplifies this dual dynamic. On one hand, AI-driven systems enable real-time threat detection, automated response mechanisms, and predictive analytics that enhance resilience against cyber incidents. Machine learning models, for instance, can identify anomalies in financial transactions during periods of economic turmoil or detect coordinated disinformation campaigns designed to destabilize political systems. On the other hand, adversaries are weaponizing AI for malicious purposes, such as generating sophisticated phishing attacks, creating deepfake propaganda to influence public opinion, or automating large-scale cyber intrusions.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

In contexts of political or economic crisis, when governance structures are already fragile, AI-powered threats could intensify instability by eroding trust in institutions, amplifying misinformation, and undermining public confidence.

Alongside AI, blockchain and Web3 technologies are reshaping the cybersecurity landscape. Decentralized architectures offer potential solutions by reducing reliance on centralized points of failure, enhancing transparency in supply chains, and creating more resilient digital ecosystems (Saleh, 2024; Karaduman, 2025). For example, blockchain-based platforms can improve trust in cross-border financial transactions during times of economic crisis, thereby mitigating risks associated with fraudulent activities (Singh & al., 2023). However, these technologies also introduce novel vulnerabilities. Smart contracts, decentralized finance applications, and digital asset exchanges are frequent targets of cybercriminal activity, resulting in significant economic losses and undermining trust in emerging digital economies (Okika et al., 2025; Qian, 2025). Moreover, the pseudonymous nature of blockchain transactions complicates regulatory oversight, facilitating illicit financial flows, ransomware payments, and even cyber-enabled terrorism (U.S. Department of the Treasury, 2022). These issues underscore the importance of governance, interoperability, and security as blockchain adoption expands within global economic and political systems (Ma et al., 2023).

An even more profound disruption on the horizon is quantum computing. While still in its early stages, quantum technologies have the potential to undermine the cryptographic foundations upon which contemporary cybersecurity rests. Widely used encryption protocols, including RSA and ECC, may become obsolete once quantum systems achieve sufficient computational power, exposing financial systems, government databases, and critical infrastructures to exploitation. This possibility is especially alarming during political and economic crises, when adversarial states or malicious actors could use quantum capabilities to destabilize already vulnerable environments. At the same time, quantum technologies may also contribute to new defensive measures, such as quantum cryptography and quantum key distribution, which promise more secure communications. Preparing for this dual-edged future will require proactive investment in post-quantum

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

cryptographic standards and international cooperation to avoid destabilizing asymmetries in technological capabilities.

Against this backdrop, the pursuit of sustainable cybersecurity strategies emerges as an urgent necessity for safeguarding global political and economic stability. Sustainable approaches go beyond technical fixes and emphasize institutional capacity building, legal harmonization, and inclusive governance. Public-private partnerships, particularly in critical sectors like banking, energy, and healthcare, will be vital to maintaining resilience during crises. At the international level, coordinated efforts to establish binding norms and frameworks could reduce the risk of cyber conflicts and foster greater trust in digital systems. Equally important is addressing structural inequalities, such as the digital divide, which leave developing economies disproportionately vulnerable to cyber threats. Investment in education, skill development, and knowledge-sharing platforms can strengthen long-term resilience across diverse geopolitical contexts. Ultimately, sustainable cybersecurity strategies must balance innovation with regulation, national interests with global cooperation, and immediate crisis responses with long-term structural preparedness, ensuring that digital vulnerabilities do not become insurmountable barriers to political and economic stability.

8. POLICY RECOMMENDATIONS

The growing entanglement of digital vulnerabilities with political and economic crises underscores the urgent need for coherent, forward-looking policy responses. Addressing these challenges requires a multidimensional approach that emphasizes international collaboration, national preparedness, public-private engagement, and equitable capacity development across the global system.

Strengthening international cooperation is vital, as cybersecurity threats are inherently transnational, often transcending borders and undermining both national sovereignty and international stability (Hassid & Matania, 2024). States must therefore intensify collaboration through multilateral institutions such as the United Nations, the G20, and regional organizations (Norm-diffusion in cyber governance: China as an emerging norm entrepreneur? 2023).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Establishing shared protocols for information exchange, coordinated incident response, and cyber threat attribution is essential to overcoming the fragmentation that currently characterizes global cyber governance (Chernenko et al., 2024; Ndubuisi, 2023). Equally important is the development of universally recognized cyber norms and confidence-building measures that can help reduce mistrust among states, mitigate the risk of escalation during crises, and foster a more stable digital environment (Lewis, 2022; Hassid & Matania, 2024).

At the national level, governments should focus on building robust cyber resilience frameworks that integrate digital security into broader security and economic planning. This entails creating centralized agencies to coordinate cyber defense, mandating sector-specific risk assessments, and embedding cybersecurity standards across critical infrastructures such as finance, energy, healthcare, and defense. Regular stress-testing of digital systems, supported by scenario-based crisis simulations, can significantly enhance preparedness for large-scale disruptions. Moreover, embedding cybersecurity into education systems and workforce development strategies will ensure a sustainable pipeline of skilled professionals equipped to manage evolving cyber threats.

Another essential recommendation is the enhancement of public–private partnerships in cybersecurity, as much of the world’s digital infrastructure is owned and managed by private corporations. Governments should incentivize private entities to adopt robust security practices through regulatory frameworks, tax benefits, and recognition schemes that reward significant investments in cybersecurity. Simultaneously, institutionalizing mechanisms for real-time threat intelligence sharing between state agencies and corporations is crucial, ensuring that confidentiality is respected while promoting collective defense. Such collaboration can not only mitigate immediate vulnerabilities but also foster innovation in advanced security technologies that benefit both national and global resilience.

Finally, particular attention must be given to capacity building in developing nations, which remain disproportionately vulnerable due to the persistence of the digital divide. International assistance programs should prioritize technical training, infrastructure development, and access to advanced cyber defense tools.

Donor countries, international organizations, and technology firms bear a shared responsibility to ensure that less-resourced nations are not excluded from global cybersecurity frameworks. In addition, regional cyber hubs can be promoted as centers of excellence, enabling knowledge transfer and collective defense strategies that enhance resilience across entire regions.

CONCLUSION

This chapter has examined the complex interrelationship between cybersecurity and digital vulnerabilities within the broader framework of international political economy, particularly in times of political and economic crises. The analysis demonstrated that cyber threats have evolved beyond isolated technical challenges and now function as critical amplifiers of systemic instability. Cyber incidents targeting critical infrastructures such as banking, energy, healthcare, and defense not only disrupt national economies but also exacerbate existing political conflicts. Case studies such as the Colonial Pipeline hack, large-scale ransomware operations, and cyber offensives linked to geopolitical tensions—including the Ukraine conflict—reveal the tangible economic costs and strategic vulnerabilities that arise from digital dependence. Furthermore, the persistence of global supply chain risks, the widening digital divide, and the particular exposure of emerging markets underscore the uneven distribution of risks and capacities in managing cyber insecurity.

By situating cybersecurity within the dynamics of international political economy, this chapter contributes to a deeper understanding of how digital vulnerabilities shape political and economic outcomes in a globalized world. It highlights that cybersecurity is not merely a technological or operational issue but a structural determinant of trust, governance, and power relations in the international system. The discussion extends existing scholarship by foregrounding the role of both state and non-state actors, including governments, multinational corporations, international organizations, hacktivist groups, and terrorist networks, in shaping the landscape of cyber risk and resilience. The chapter further underscores the fragmented nature of global cyber governance and the absence of universally binding norms, which collectively limit the capacity to address cross-border cyber threats effectively.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

By drawing attention to the interplay of economic fragility, political instability, and digital interdependence, this work enriches the theoretical and policy-oriented dimensions of international political economy studies.

Looking ahead, the future of cybersecurity in the context of political and economic crises will be shaped by both the opportunities and risks emerging from disruptive technologies such as artificial intelligence, blockchain, Web3 infrastructures, and quantum computing. These innovations hold the potential to enhance resilience, transparency, and efficiency, yet they also introduce new vulnerabilities and avenues for exploitation.

Strengthening international cooperation, promoting cross-sectoral collaboration between public and private actors, and investing in capacity-building—especially in developing regions—remain central to mitigating these risks. Ultimately, cybersecurity must be recognized as a foundational element of stability in the international political economy. By treating digital vulnerabilities as structural forces rather than isolated technical issues, policymakers and scholars alike can better anticipate the challenges of future crises and craft strategies that safeguard both economic systems and political legitimacy.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

REFERENCES

Accenture. (2025). State of cybersecurity resilience 2025. <https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf>

African Union. (2014/2023). African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention). <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

AInvest. (2025). Geopolitical cybersecurity risks and emerging market opportunities: Strategic investment analysis. AInvest.

Andini, N. K. T., Damayanti, N. M. A. P., & Purnama, N. K. W. (2023). Cybercrime and threats to the electoral system. *International Journal of Government and Information Systems*.

ASEAN. (2022). ASEAN cybersecurity cooperation strategy 2021–2025. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Baldoni, R., & Di Luna, G. (2025). Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities. *arXiv*. <https://doi.org/10.48550/arXiv.2503.10140>

Beyer, J. L. (2023). The politics of cybersecurity and the global Internet. *Perspectives on Politics*. <https://doi.org/10.xxxx/xxxxx>

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity-building. *Third World Quarterly*, 41(6), 917–938. <https://doi.org/10.1080/01436597.2020.1729729>

Canadian Centre for Cyber Security. (2024). Cyber threats to Canada's democratic process. *Government of Canada*. <https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process>

Chernenko, E., Demidov, O., & Lukyanov, F. (2024). Increasing international cooperation in cybersecurity and adapting cyber norms. *Council on Foreign Relations*.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Cyberly. (2024). How do ransomware attacks impact critical infrastructure? <https://www.cyberly.org/en/how-do-ransomware-attacks-impact-critical-infrastructure/index.html>

Delphos Cybersecurity. (2025). Cybersecurity in emerging markets: Protect your business. Delphos.

ENISA (European Union Agency for Cybersecurity). (n.d.). What we do: Empowering communities – operational cooperation – capacity building. <https://www.enisa.europa.eu/about-enisa/what-we-do>

European Commission. (n.d.). Legal framework of EU data protection. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

European Commission / Digital Strategy. (n.d.). NIS2 Directive: Securing network and information systems. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

Gomez, M. A., & Shandler, R. (2022). Cyber-conflict and the erosion of trust. Council on Foreign Relations Blog. <https://www.cfr.org/blog/cyber-conflict-and-erosion-trust>

Hassid, N., & Matania, E. (2024). A global regime for cybersecurity and the obstacles to future progress. *Global Governance: A Review of Multilateralism and International Organizations*, 30(1), 13–40.

Heeks, R. (2021). From digital divide to digital justice in the Global South: Conceptualising adverse digital incorporation. arXiv. <https://arxiv.org/abs/2108.09783>

Hendin, R. (2020). Cyber-enabled foreign interference in elections and referendums. Australian Strategic Policy Institute.

IBM Institute for Business Value. (2024). How cybersecurity shapes supply chain resilience. IBM.

International Telecommunication Union. (2024). Global strategic report: Roles and responsibilities for digital security. https://www.itu.int/osg/csd/cybersecurity/gca/docs/global_strategic_report.pdf

Iyengar, V., & Lukasik, S. (2024). What is cyber-warfare? S&P Global Market Insights.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Karaduman, Ö. (2025). Blockchain-enabled supply chain management: A review. *Applied Sciences*, 15(9), 5168. <https://doi.org/10.3390/app15095168>

Konecka, S., & Bentyn, Z. (2024). Cyberattacks as threats in supply chains: A bibliometric and case-study analysis. *European Research Studies Journal*, 27(3), 778–796.

Kshetri, N. (2016). Cybersecurity and development: Issues and implications for the Global South. *Markets, Globalization & Development Review*, 1(2), Article 3. <https://doi.org/10.23860/MGDR-2016-01-02-03>

Ma, W., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). A comprehensive study of governance issues in decentralized finance applications. *arXiv*. <https://arxiv.org/abs/2311.01433>

Maurer, T. (2021). The global cyber threat to financial systems. International Monetary Fund, *Finance & Development* (March).

Maurer, T. (2022). The promises and perils of a minimum cyber deterrence posture: Considerations for small and middle powers. Hague Centre for Strategic Studies. <https://hcss.nl/wp-content/uploads/2022/04/Cyber-Deterrence-Final.pdf>

Ndubuisi, A. F. (2023). Strengthening national cybersecurity policies through coordinated threat intelligence sharing and real-time public-private collaboration frameworks. *International Journal of Science and Research Archive*, 8(02), 812–831.

Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cybersecurity strategies of ten nations. *arXiv*. <https://doi.org/10.48550/arXiv.2303.13938>

OECD. (2025). Economic security and vulnerabilities in international supply chains. OECD Publishing. <https://doi.org/10.1787/4eac89c7-en>

Organisation for Economic Co-operation and Development. (2019). Roles and responsibilities of actors for digital security (OECD Digital Economy Papers No. 277). OECD Publishing.

Parikkar, C. S. (2024). Digital world: Threats to security and the scope for South–South cooperation. *Artha Journal of Social Sciences*, 55(2). <https://doi.org/10.12724/ajss.55.2>

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Paulis, E. (2025). The flip side of digital technologies in internal party elections. *Journal of Contemporary Governance*.

Qian, P. (2025). Comprehensive review of smart contract and DeFi security. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2025.02.0500>

Romavella, A. B. A. P. (2024). Cyberattacks on government-managed systems through the lens of social epistemology. *Journal of Social Epistemology and Cyber Governance*.

RUSI. (2024). Ransomware now threatens the Global South. Royal United Services Institute.

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence: A systematic literature review. *Computers & Electrical Engineering*. <https://doi.org/10.1016/j.compeleceng.2024.006X>

Shandler, R., Gross, M. L., & Canetti, D. (2023). Trust at risk: The effect of proximity to cyberattacks. *Journal of Information Technology & Politics*, 20(4), 359–374. <https://doi.org/10.1080/19331681.2022.2112796>

Singh, R. K., et al. (2023). Blockchain applications for secured and resilient supply chains. *Computers & Industrial Engineering*. <https://doi.org/10.1016/j.cie.2022.10.100>

Stepan, O., & Trushkina, N. (2025). The geopolitics of cybersecurity: A comparative analysis of national strategies for digital sovereignty. *Politics & Security*, 12(2), 59–71. <https://doi.org/10.54658/ps.28153324>

Timcke, S., Gaffley, M., & Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication*, 32, 1–28. <https://doi.org/10.23962/ajic.i32.16949>

Tuteja, A. (2025). Cybersecurity: 5 risk factors from supply chain interdependencies. World Economic Forum.

U.S. Department of the Treasury. (2022). Illicit finance risk assessment of decentralised finance. <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

UNCDF. (2024). The role of cybersecurity and data security in the digital economy. *Policy Accelerator*.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

<https://policyaccelerator.uncdf.org/all/brief-cybersecurity-digital-economy>

World Bank. (2023). Cybersecurity in financial sector development: Challenges and potential solutions for financial inclusion. World Bank.

World Bank. (2024). Cybersecurity economics for emerging markets. <https://documents1.worldbank.org/curated/en/099091624175097991/pdf/P17876915bd69a0671b2f2166697a1c7793.pdf>

World Economic Forum. (2022). Chapter 3: Digital dependencies and cyber vulnerabilities. In The Global Risks Report 2022. World Economic Forum.

World Economic Forum. (2024). Global Cybersecurity Outlook 2025: Understanding complexity in cyberspace. <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/1-understanding-complexity-in-cybersecurity-587e8c5eba>

Kennan Institute / Harvard Kennedy School. (2018, February 15). The state and local playbook 1.1–2: Election system overview: Potential attack vectors. <https://www.belfercenter.org/sites/default/files/2024-08/StateLocalPlaybook%201.1-2.pdf>

World Economic Forum. (2019, August). We must treat cybersecurity as a public good. <https://www.weforum.org/stories/2019/08/we-must-treat-cybersecurity-like-public-good/>

Chatham House. (2019, December). The application of international law to state cyberattacks: Application of the law to case studies. <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/4-application-law-case-studies>

Maurer, T., & Nelson, A. (2021, March). The global cyber threat to financial systems. IMF – Finance & Development. <https://www.imf.org/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems>

Lewis, J. A. (2022, February 23). Creating accountability for global cyber norms. Center for Strategic and International Studies (CSIS).

Rajagopalan, R. P. (2023, January 29). Space and cyber global governance: A view from the Global South. Centre for International Governance

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Innovation. <https://www.cigionline.org/articles/space-and-cyber-global-governance-a-view-from-the-global-south/>

Jindal, D. (2023, January 31). Geopolitics of cyber attribution. Vivekananda International Foundation. <https://www.vifindia.org/article/2023/january/31/geopolitics-of-cyber-attribution>

Adrian, T., & Ferreira, C. (2023, March 2). Mounting cyber threats mean financial firms urgently need better safeguards. International Monetary Fund. <https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards>

World Economic Forum. (2023, April 21). How tech is creating vulnerabilities in the financial system. WEF Agenda.

OpenGov Asia. (2023, September 19). ASEAN cybersecurity: The need for public-private partnerships. <https://archive.opengovasia.com/2023/09/19/asean-cybersecurity-the-need-for-public-private-partnerships>

BAE Systems. (2024, February 20). The cyber impact on elections: Safeguarding democracy in 2024. <https://www.baesystems.com/en/insight/the-cyber-impact-on-elections-safeguarding-democracy-in-2024>

McKinsey & Institute of International Finance. (2024, March 11). The cyber clock is ticking: Derisking emerging technologies in financial services. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services>

Lemos, R. (2024, March 26). Africa tackles online disinformation campaigns during major election year. Dark Reading.

BigID. (2024, December 20). 46% of financial institutions had a data breach in the past 24 months. Help Net Security. <https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/>

World Economic Forum. (2025, January 10). Global Cybersecurity Outlook 2025.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

World Economic Forum. (2025, January 13). Global Cybersecurity Outlook 2025 – Navigating through rising cyber complexities [Press release]. <https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/>

OSTI. (2025, April). Strategic competition in cyberspace: Hard and soft cyber means in state conflict and power. U.S. Department of Energy. <https://www.osti.gov/servlets/purl/1635774>

Kalash, A. (2025, June). Cyber risk and global financial systems (CIGI Paper No. 324). Centre for International Governance Innovation. https://www.cigionline.org/static/documents/no._324_Kalash.pdf.

CHAPTER 2
CLIMATE CHANGE AS AN ECONOMIC AND
POLITICAL CRISIS

Huzaifa AHMAD¹

¹ huzaifa@lutar.my, WhatsApp: ORCID ID: 0009-0002-4135-6460.

INTRODUCTION

The nexus of the global economic and political systems and climate change has become one of the characteristics of the modern international political economy (IPE). Climate change is no longer an environmental concern but a mainstream issue that economists, political scientists, and policy-makers must handle when dealing with its extensive ramifications on the world's stability, development, and governance (Babic & Sharma, 2023). It was a year of several landmark events in this developing crisis, with all-time high global temperatures and unprecedented economic damage due to weather events, reaching its peak with the COP29 climate summit that highlighted the seriousness of the crisis alongside the ineffectiveness of the current response.

The thesis of this chapter is that change has to be perceived as an essential crisis of an essential nature, both economic and political, that affects growth, development, and governance within the international system. The financial aspects occur in the form of direct costs of the impacts of climate, stranded assets in the fossil fuel sectors, and the enormous financial needs of mitigation. According to recent estimates, climate change may cut the world's GDP by 12 percent per degree of warming, and extreme weather has already destroyed the global economy of more than \$2 trillion in the last ten years (World Economic Forum, 2024).

At the same time, climate change is a significant political crisis, which reveals the weaknesses of current forms of governance, democratic practices, and international collaboration schemes. The results of COP29, which set a 300 billion annual climate finance goal by 2035, well below the 1 trillion requested by developing countries, are a source of the ongoing political obstacles to proper climate action (UNFCCC, 2024).

The theoretical model used to analyze this issue is based on critical ideas on IPE that explore the interrelations among economic systems, political influence, and environmental pollution. Placing climate change in the broader context of global capitalism, governance, and global inequality, this chapter becomes a part of the current literature that puts the environmental issues at the focus of IPE analysis, instead of analyzing them as an externality.

1. THEORETICAL BACKGROUND: CLIMATE CHANGE IN THE IPE BACKGROUND

To comprehend climate change as a political economy crisis, it is important to have a theoretical framework capable of embracing intricate interactions between environmental working, economic systems, and political structures. Conventional IPE methods, which have mainly emphasized tradefinance and pr, have been unable to adequately incorporate the environmental aspects (Tanner & Allouche, 2011). Nevertheless, in the current trends in critical IPE research, these attempts have developed more detailed frameworks that theorize environmental degradation as a product and a cause of more general political-economic processes.

Climate Crisis and Historical Materialism

Historical materialism theories of IPE offer a background knowledge of how climate change results from the contradiction of capitalist accumulation. The ideology of unlimited expansion on a limited planet establishes the so-called second contradiction of capitalism, as defined by O'Connor (1998), which is that the capitalist production mode is self-destructive regarding the environmental conditions of its existence. This model assists in describing the reason why the market-based approaches to the issue of climate change, including carbon trading and green finance, fail to deal with the underlying factors of environmental degradation and continue to provide new possibilities for capital accumulation.

This analysis is further expanded to the international level, and the concept of ecological imperialism looks at how climate change reflects global inequalities and confirms them. The developed nations have contributed unevenly to the historical emissions. In contrast to the least developed nations, the highest effects of climate change result in so-called slow violence against the global poor, as explained by Nixon (2011). This model sheds light on the continued failure of climate finance talks to address the needs of the vulnerable nations because it undermines the current trends of global wealth distribution.

Climate Politics and Governance Theory

In a governance approach, climate change poses a regime complex, which Keohane and Victor (2011) define as a loosely coupled system of institutions and agreements that frequently operate at cross-purposes. The divisiveness of climate governance between levels and actors poses coordination issues that hinder effective activity. The recent COP29 experience illustrates such difficulties because the negotiation could not effectively balance competing national interests, sectoral interests, and time horizons.

Democratic deficits in climate governance have increasingly come into focus as climate policies are costly to the present generations of people to benefit those who will only reap the benefits to come in other nations and generations that will be born later. The result of this time-space disengagement between the costs and benefits of climate change is a so-called perfect moral storm (Gardiner, 2011) that complicates the conventional method of accountability for democracy.

Financial, Political Economy and Climate Risk

Introducing climate concerns in financial markets is a new frontier of IPE analysis. Also identified as a key issue of financial stability is the concept of stranded assets, which, in other words, are investments that will lose their value because of climate policy or the physical effects of climate (Daumas, 2024). As the shift to a low-carbon economy threatens financial institutions and pension funds worldwide, they may have to deal with estimates of up to 1.3 trillion of fossil fuel reserves left stranded behind under draining climate policies.

The emergence of green finance and environmental, social, and governance (ESG) investing has brought about novel types of financialization, which are trying to reconcile market incentives and environmental goals. Nevertheless, according to the critical scholars, these strategies can also assist in producing new methods of green grabbing where nature is commodified without solving the leading causes of environmental degradation (Bracking, 2015).

2. CLIMATIC CRISIS ECONOMIC DIMENSIONS

Climate change has economic repercussions much wider than direct expenditures on extreme weather events, including structural changes in worldwide production, commerce, and finances. These two economic aspects can only be understood by looking at the short-term expenses of the effects of climate change and the overall structural adjustment necessary for decarbonization.

The Direct Economic Costs of Climate Change

Recent studies have strongly adjusted the upward estimates of economic costs of climate change. A 2024 study that examined in detail revealed that every one degree of increased global warming would decrease global GDP on average by about 12 to 12 percent, which is considerably more than earlier estimates had been between 1 and 3 percent (World Economic Forum, 2024). The revision also represents a better grasp of the effects of climatic factors on productivity, infrastructure, and human conditions, as well as the modeling of extreme weather and breaking points. Economic costs are experienced in various ways. The indirect effects of physical climate are the rising sea level, increased heat, drought, and floods, which directly harm infrastructure, lower agricultural output, and interfere with supply chains. The International Chamber of Commerce has estimated that the world economy incurs over two trillion dollars annually because of extreme weather over the last ten years, and the costs have been growing at an alarming pace in recent years (ICC, 2024). Another important means of economic influence is labor productivity. The increased temperatures lead to less productivity, especially in the outdoor industries like agriculture and construction. A report by the International Labour Organization discovered that heat stress could decrease working hours worldwide by 2.2 per cent by 2030, which is 80 million full-time working positions. This has a very harsh economic effect in developing countries, whereby outdoor work forms a greater percentage of the employment.

Stranded Assets and Transition Costs

A low-carbon economy needs large-scale investments in clean energy, energy efficiency, and sustainable infrastructure.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Clean energy investments of \$4.4 trillion annually worldwide, a complete re-direction of the capital flows, are estimated by the International Energy Agency as necessary to have net-zero emissions by 2050. Such a transition presents opportunities in various industries and areas. The notion of stranded assets has become the most important for the economic aspect of climate transition. There is the prospect that fossil fuel companies will be unable to burn proven reserves within carbon budgets used to achieve warming of less than 1.5 °C or 2.2 °C. According to the Bank of International Settlements, it is estimated that up to 20 trillion of fossil fuel wealth might be stranded under severe climate policies, with it representing a serious threat to the financial stability (BIS, 2023). The geographic allocation of stranded assets forms new economic inequality. The oil-based economies have specific problems with their economic base diversification, whereas the areas with a high concentration of renewable energy sources might take advantage of the transition. This new geography of energy generates new patterns of economic advantage and disadvantage, making international climate negotiations more difficult.

Climate Finance and Development

Financing climate action in developing countries constitutes one of the most debatable matters of international climate policy. The principle of common but differentiated responsibilities by the UNFCCC acknowledges that the developed nations have a moral duty to give the developing nations financial aid in mitigation and adaptation activities. Nevertheless, the amount of finance availed has always been short of the needs evaluated. The COP29 agreement to churn up \$300 billion by 2035, compared to the old target of \$100 billion, may be seen as an improvement over the old target. However, it is still far below developing countries estimated annual climate financing requirements (UNCTAD, 2024).

The distance between the demands and the commitments indicates the size of the problem and the political opposition to extensive financial transfers. Debt sustainability and economic sovereignty also become issues of concern because of the climate finance framework. Many climate finance is in the form of loans and not grants. This is likely to increase the debt levels in countries already strained financially.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The focus on mobilization of the private sector via the use of blended finance schemes can focus on commercially viable projects rather than on adaptation efforts that will yield minimal financial benefits but produce necessary public goods.

3. APOLITICAL ASPECTS AND GOVERNING FAILURES

The political aspects of the climate crisis are also more indicative of the underlying difficulties in international governance, democracy, and collaboration. Climate change brings about new patterns of political struggle and brings out the shortcomings of the prevailing institutional provisions to the global collective action problems. Democratic deficits in climate governance have been identified in structures, procedures, and resources, especially within the EU, the USA, and the UK.

Democratic Deficits in Climate Governance Structures

Procedure and resources have been found to have democratic deficits in managing climate, particularly in the EU, the USA, and the UK. Climate change brings fundamental issues of democratic governance because of its spatial and temporal nature. The cost of climate action falls primarily on contemporary voters and domestic interest groups, whereas future generations and the populations of other nations share the benefit.

This generates a so-called democratic deficit of climate policy by political scientists because electoral incentives usually cut across long-term thinking essential to successful climate action. The emergence of climate activism, especially among the youth, can be attributed to the above democratic lapses. Fridays for Future and Extinction Rebellion movements believe that the legacy of democracy has not been able to effectively reflect the interests of future generations and the population at risk due to climate change. The rising trend of climate litigation, which has seen more than 2,000 climate lawsuits filed worldwide, indicates efforts to have the judicial mechanisms overcome the law-making systems of silence on climate change. Nonetheless, the attempts to shield the climate policy against democratic demands with the help of technocratic organizations and international treaties do generate their own legitimacy issues.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The democracy versus climate dilemma that is evidence of more fundamental conflicts in liberal democratic theory regarding how to resolve collective action problems of long-term systems operating under systems of short-term political competition.

Free-Riding and International Cooperation.

Climate change is a typical global problem of public goods, with the advantages of emissions cut felt worldwide, whereas the disadvantages are faced in the home country. This motivates free-riding because nations will benefit from other nations' climate efforts without making efforts towards mitigation. A long history of international climate negotiations has been characterized by endemic tensions between nations that want to maximize their individual economic benefits at a minimum cost to their commitments on climate. The Paris Agreement tried to solve these cooperation issues by utilizing a nationally determined contribution (NDCs) system that will enable countries to establish their own targets, but in a manner that places peer pressure on them to take ambitious action. However, because the system is voluntary, the will to limit warming to 0.5 °C (and 2 ° 2degC), there is an ambition gap between what is promised and what is actually done by current NDCs. The COP29 results demonstrate the unresolved issues in global climate collaboration. Although there is scientific evidence of accelerating climate effects and increasing public awareness on the issue of climate change, the talks were still at a stalemate in fundamental responsibility, capability, and the sharing of questions. The pledge to increase climate funds to triple to \$300 billion annually is a step in the right direction, but not a transformational step that climate science says it needs to take.

Regulatory Capture and Corporate Power.

Fossil fuel industries are one of the biggest obstacles to successful climate action. Although there is an increasing realization of the dangers of climate change, fossil fuel corporations remain very influential in the political sphere with lobbying, campaign contributions, and the revolving door between the industry and government.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The fact that more than 2,400 representatives of the fossil industry are at COP29, more than in some countries, reflects the political sway of the carbon-intensive industries. The regulatory capture concept helps understand why climate policies are usually less effective than science recommends. The oil companies have managed to manipulate the policy design in such a way that they reduce the costs of their industries to put the strains on the consumers and taxpayers. The dominance of voluntary methods, market-based policy, and the phase-out methods indicates industry influence on policy formulation. Nevertheless, renewable energy industries and green technology firms have emerged, and they have started forming new political alliances in favor of climate action. Recent dramatic electricity cost-cuts in solar and wind energy have rendered clean energy a competitor of fossil fuels, generating constituencies of businesses in favor of supportive policies. This changing economic interest balance can assist in breaking a few of the political divides of climate action.

4. THE ECONOMIC INTERSECTION OF ECONOMIC AND POLITICAL CRISES

Climate change has strong economic and political aspects that mutually supporting and enhance each other, making the systems vulnerable and governance difficult. The fact that these intersections exist, and learning about them is essential in addressing the climate crisis.

Climate Change and Economic Inequality

Climate change is a manifestation and a confirmation of current trends of economic inequality both within and between nations. The most vulnerable groups are generally the poorest with the least adaptive capacity and are usually vulnerable to climate risks. This forms a vicious cycle in which climate effects exacerbate inequality, further decreasing social cohesion and political backing to take action on climate. There is a skewed allocation of climate effects and adaptation at the global scale, so-called climate apartheid (Roberts & Parks, 2007). Small island developing nations have an existential risk of rising sea levels, even though their contribution to global emissions is less than 1 percent.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

In contrast, large emitters like the United States and the European Union have more opportunities to implement climate change response strategies. Such disparity subverts the credibility of worldwide climate governance and creates disputes over responsibility and burden-sharing. The retrogressive character of most climate policies complicates these inequality issues. Carbon and energy prices impact low-income households more, and subsidies on electric cars and solar panels mainly cover middle and upper-income groups. The protests of the yellow vests in France and similar events in other countries reveal that climate policies can become an arena of deep-rooted social struggles against inequality and economic justice.

Financial Instability and Systemic Risk

Climate change causes additional forms of systemic risk in the global financial system due to both physical climate risks and transition risks. Physical risks involve direct losses to assets through extreme weather conditions, whereas transition risks involve policy changes and technological flip-flops that influence the value of assets. The fact that global financial markets are interconnected implies that the losses caused by climate change can swiftly spread through institutions and borders.

Climate change has become a recognized area of financial stability risk to central banks and other financial regulators. The Bank for International Settlements has encouraged that climate change may spark the next financial crisis unless well-managed, and the European Central Bank is already adding climate hazards to its stress testing processes. Nevertheless, climate risks are also complex to evaluate with the help of the conventional risk management instruments, which are not focused on the long-term.

The idea of a green swan event, a climate-related shock that would cause extensive financial instability, has become known among policy-makers and risk managers. Green swan events are predictable but hard to prepare against, unlike the traditional black swan events, which are unpredictable. However, they are predictable because of their unprecedented nature and interactions between them and economic and political systems.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Resources Brawl and Geopolitical Unsteadiness.

Climate change has several impacts on geopolitical stability, which include the lack of resources, human displacement, and economic power movement. Conflicts arising due to natural resource scarcity may include natural resource stress, deteriorating earning power of agricultural activities, and natural disasters, especially in areas with fragile establishment and where tensions already exist.

Climate change has generated security implications that have been understood by the military and intelligence agencies around the globe. The U.S. Department of Defense has recognized climate change as a threat multiplier, which increases security challenges, and NATO has seen climate change as one of the challenges of the 21st century. Nevertheless, the securitization of climate change can also lead to the militarization of action and the negation of human security strategies based on adaptation and resilience.

Another overlap of economic and political aspects is climate-induced migration. The Internal Displacement Monitoring Centre estimates that were 32.6 million displaced in 2022 due to weather-related disasters, with the majority of this movement being within countries and not across boundaries. Although climate migration has the potential to offer economic opportunities and decrease vulnerability, it may also place a strain on available resources in the destination regions and cause political tensions related to immigration and integration.

5. CASE STUDIES AND MODERN DAY

A detailed analysis of specific examples of climate-based economic and political crises offers practical examples of the theoretical models and overall trend covered by the discussions above. This part compares three recent occurrences, illustrating various facets of climate change as a political-economic crisis.

European Energy Crisis and Climate Policy.

The European energy crisis that started in 2021 and only escalated due to the Russian invasion of Ukraine demonstrates how policy on climate, energy security, and economic stability are complexly related.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The reliance of Europe on Russian gas posed weaknesses that had been revealed when the geopolitical tensions disrupted supply chains, causing mass panic and fears of energy rationing. The crisis showed the tension between short-term energy security and long-term climate goals. European nations have temporarily increased coal consumption and postponed the shutdown of nuclear plants. Went further to hasten the use of renewable energy to promote energy self-sufficiency. In May 2022, the plan was announced as REPowerEU, which aimed to stop European reliance on Russian fossil fuels by 2030 through energy savings, diversification, and hastening the implementation of renewable energy. The energy crisis posed severe political difficulties because of its distributional effects. Industries that consume energy were being cut down in production, and the possibility of closing down plants, families were finding it tough to cope with the increased costs of heating and electricity. The response by governments was enormous subsidy programmes of estimated costs exceeding EUR700 billion throughout the EU that served to stabilize political conditions but cast doubt on financial sustainability and the incentives to energy efficiency in the long run. The eventual rush caused by the crisis facilitated the transition to clean energy in Europe because it showed the benefits of energy security through independence on renewable energy. It, however, also pointed to the political economy problems of dealing with transitions and not relying on fossil fuels, especially the necessity to deal with distributional effects and keep the population on side when the economy was under pressure.

Loss and Damage in Small Island Developing States

The case study of climate vulnerability and politics of loss and damage in Small Island Developing States (SIDS) is fascinating. It is also existential since high sea levels, coastline erosion, and more frequent and destructive tropical cyclones affect these countries. However, they contribute less than 1 percent of all the greenhouse emissions worldwide. Their contribution to the problem is minimal, and at the same time, they are highly vulnerable, making the core of the inequity of climate change. Creating a Loss and Damage Fund in COP27 in 2022 was a significant political triumph of SIDS and other vulnerable nations, who had been promoting the establishment of a mechanism like that for over 20 years.,

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Nonetheless, it has been difficult to operationalize the fund, with disputes as to its funding source, governance modes, and eligibility. The original pledges of 700m are way below the estimated requirements of 130-940 billion in 2025 alone (IIASA, 2024). The example of Tuvalu shows how high the challenges are for low-lying island states. Tuvalu is submerged under the sea-level rise scenarios of 4.6 meters above sea level. The government has prepared some contingency planning for possible population relocation and recommended an international lawful recognition of the so-called disappearing states that would still enjoy sovereignty despite the territory becoming uninhabitable.

Economic effects of climate change in SIDS go beyond direct physical losses to include adverse effects, such as diminished tourism, projects in the fishing industry, and agricultural produce. Coral bleaching, coastal erosion, and extreme weather events have threatened the tourism industry, a source of significant foreign exchange to many of the SIDS. Interdependence of the small island economies implies that the effects of climatic conditions in one sector spread very fast to the entire economy.

Climate Finance and Debt Distress in Africa.

The climate finance challenge is experienced in Africa in a very acute form because the countries need to make considerable investments in adaptation and mitigation, as well as work with the existing debt burden and constrained fiscal space. The continent is the source of only 4% of the world's greenhouse gas emissions, although some of the worst climate effects are experienced, which forms the basis of unfairness in the causes and effects.

Due to its structure, climate finance has contributed to the debt sustainability problem in most African countries. Climate finance is mainly in the form of loans rather than grants, contributing further to the debt burdens in the countries where the government debt-to-GDP ratio has already significantly increased. The IMF approximates that 22 African nations are either in a state of debt distress or in high danger of debt distress, constraining them from investing in climate resilience. The experience of climate finance in Kenya depicts both opportunities and challenges. The country has been relatively prosperous regarding international climate finance access, as it has received more than 3 billion climate-related funds since 2010.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

However, much of this funding has been in the form of loans, which leads to the country's debt burden, with the emphasis on mega infrastructure projects often supplanting the community-based adaptation methods. The recent debt restructuring talks between Zambia, Ghana, and other African nations have started to include climate factors, with the creditors agreeing to write off debt as long as these nations promise to act on climate. These debt-for-climate swaps are a new methodology for dealing with the convergence between debt and climate issues, but are very small compared to aggregate funding requirements.

6. IMPLICATIONS AND FUTURE DIRECTIONS OF THE POLICY

The climate change as an economic and political crisis analysis is leading to some core policy implications, research, and action directions in the future. This will involve radical changes in economic systems and governance frameworks instead of incremental modifications to deal with the climate crisis.

Economic Systems Transformation

Compared to economic systems, the scale and urgency of the climate crisis demand fundamental changes and not marginal adaptation to current methods. Degrowth has become popular as an alternative to growth-based models, which might not align with planetary boundaries. Nevertheless, implementing the degree of growth methods has many political and practical obstacles, especially concerning jobs and growth in less developed nations.

An even better solution can be defining growth differently and dwelling, being, and sustainability instead of material throughput. Creating alternative economic measures, like Gross National Happiness or the Genuine Progress Indicator, gives rubrics on how economic success can be gauged beyond GDP growth. Costa Rica and Bhutan are some countries that have started to put measures like these in their policy frameworks. Shifting to a circular economy is another way to align economic activity with environmental constraints. Circular economy solutions may minimize resource usage and still deliver economic activity by designing waste out and holding products and materials in circulation.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Nevertheless, the future of circular economy methods is achievable through massive investments in new infrastructure, business models, and policy frameworks that internalize the environmental costs.

Reforming Global Governance

The weakness of the existing international climate governance institutions demands radical changes in the global governance setups. UN climate negotiations, using a consensus, have failed to provide the speed and magnitude of action that climate science needs. Other strategies, like using climate clubs by willing states or special-purpose governance facilities, can offer more promising avenues of action on climate. Another significant reform direction is the democratization of global rule. The existing framework in the international climate negotiations offers few avenues to the civil community, future generations, and the population at risk to engage in the process. Citizens' assemblies, including young people in international negotiations, and granting future generations legal status can be some innovations that could amend these democratic deficits.

There can also be an increasing role of regional and sub-national levels of governance in climate action. Cities, states, and regions can innovate new policies more quickly than national governments or even offer intermediate degrees of coordination, which do not entail all the difficulties of global governance, especially regional organizations. The C40 Cities Climate Leadership Group and other networks portray the potential of multi-level climate governance.

Meeting Justice and Equity

The equity aspects of climate change demand a clear focus on the distributional effects and procedural justice during climate policy formulation. One conceptual framework for addressing decarbonization's social costs is Just transition frameworks that support workers and communities reliant on fossil fuel industries. Nevertheless, just transition strategies must not only focus on remuneration but also be extended to include a time of involvement in decision-making and diversifying the economy.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Climate reparations are a more extreme measure to solve past injustices regarding climate contributions and impacts. Climate reparation proposals generally entail massive financial flows between high-emitting developed nations and climate-sensitive developing nations, premised on the principles of corrective justice over historic emissions. Despite the political difficulties, climate reparations structures offer valuable normative principles to conceptualize climate justice.

Another significant equity issue is incorporating climate policy and indigenous knowledge and rights. Indigenous peoples are stewards or tenure holders of one-fourth globally, and sustain nearly 80 percent of global biodiversity, whose experience and involvement will be vital to successful climate action. Nevertheless, the indigenous peoples tend to be excluded from the climate policy processes, although they are disproportionately affected by climate change.

Institutional Innovation

The change in climate as a crisis of political economy needs new institutional arrangements that will be able to handle the complex relationships between economic, political, and environmental systems. An institutional innovation in this area is green central banking, where central banks are starting to put climate risks into their monetary policy and financial regulation. Nevertheless, central bank climate action continues to be controversial regarding the correct scope of appropriate central bank intervention, and there are fears of democratic accountability and mission creep.

Climate courts and legal innovations offer another source of institutional development. The increasing number of climate litigation cases has established new areas of legal precedence and compelled governments to defend against poor climate performance. The rights of nature and the legal standing of future generations are even more radical legal innovations that can change how environmental governance is undertaken.

The deliberative and participatory institutions provide opportunities to overcome democratic gaps in climate governance. In some countries, citizens' assemblies about climate change have been created and have typically made recommendations for more ambitious climate action than the everyday politics.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

These experiences indicate that the obstacles to climate action politicians encounter can be overcome by providing citizens with information and deliberation opportunities.

CONCLUSION

This chapter has discussed climate change as an economic and political crisis that undermines the current provision of the international political economy. The discussion has shown that climate change should not be perceived merely as an environmental issue that needs technical solutions, but as a systemic crisis that reveals profound contradictions of the accumulation of capital, democratic regimes, and global collaboration.

The economic aspects of the climate crisis go way beyond the cost of the extreme weather events, directly to the core issues concerning growth, development, and financial security. As the most recent estimates indicate a 12-percent decrease in global GDP with a 1 °C of warming, climate change presents unparalleled challenges to economic systems based on predictions of unlimited growth and environmental stability. The losses to the economies associated with extreme weather of up to 2 trillion in the last ten years are a preview of the bigger economic losses in the future, in the case of further emissions along the same lines.

Political aspects are also profound because climate change brings about new conflict modalities and also reveals the weakness of the current governance systems. The democratic weaknesses attendant to climate policy in the form of immediate costs and distant benefits cast the fundamental assumptions of democratic responsibility and representation in a negative light. The results of COP29, in which a climate financing deal representing 300 billion US dollars was well below the estimated 1 trillion of financing the challenge, can be seen as a reflection of the incumbent inadequacy of the existing political institutions to meet the challenge with sufficient strength.

The overlap of economic and political crises generates structural weaknesses that threaten local and global stability. Climate change exacerbates the existing inequalities and creates new manifestations of economic and political turmoil that do not correspond to the classic methods of development, security, and international collaboration.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The case studies in the European energy crisis, loss and damage in small island states, and debt distress in Africa show the spread of climate effects by the interconnected economic and political systems in a manner that is hard to foresee and control. Climate change is a crisis in the political economy, and transformative changes beyond incremental reforms must be addressed. The analysis identifies several critical directions of future action, namely to transform economic systems to function within planetary boundaries and to change global governance to adapt to democratic deficits and power imbalances, to focus justice and equity in designing climate policies, and to create new institutional arrangements capable of managing complex socio-ecological systems.

The pressing nature of the climate crisis implies that such changes must be made as soon as possible within that small window of opportunity to ensure that warming is limited to comparatively safe ranges. The political economy study, however, also brings to our attention why such changes are hard to implement in the prevailing institutional setups. The question posed to theorists and practitioners of international political economy lies in devising new models and strategies that would be able to operate within this tension between the necessity and the political expediency.

Further studies need to be devoted to creating more complex methods to examine the complicated relations between climate change, economic, and political systems. This involves considering possible alternative financial systems, new forms of governance, and groundbreaking policy responses capable of dealing with climate change and ensuring social justice and democratic involvement. Climate crisis is not only a root cause of discontinuity in the current order of the world's international political economy, but also a chance to come up with more sustainable and fairer alternative solutions.

The stakes were not high enough. The decisions that will be made during the coming years in terms of economic mechanisms, governmental structures, and global collaboration will significantly influence whether humanity will be able to escape the most devastating effects of climate change whilst constructing more rightful and peaceful communities.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The concept of climate change as a crisis of political economy offers the necessary encouragement to make such crucial decisions and to work out the answers that would be sufficient to the magnitude and urgency of the situation we have to deal with.

REFERENCES

Babic, M., & Sharma, S. E. (2023). Mobilising critical international political economy for the age of climate breakdown. *New Political Economy*, – 28(3), 315-333.

Bank for International Settlements. (2023). *Climate-related financial risks: A survey on current initiatives*. BIS Papers No. 128.

Bracking, S. (2015). The anti-politics of climate finance: The creation and performativity of the green climate fund. *Antipode*, 47(2), 281–302.

Daumas, L. (2024). Financial stability, stranded assets, and the low-carbon transition—A critical review of the theoretical and applied literatures. *Journal of Economic Surveys*, 38(1), 169-203.

Gardiner, S. M. (2011). *A perfect moral storm: Climate change and intergenerational ethics*. Oxford University Press.

International Chamber of Commerce. (2024). *Economic impact of extreme weather events: Global assessment 2024*. ICC Research Foundation.

International Institute for Applied Systems Analysis. (2024). Loss and damage funding requirements for vulnerable countries: 2025 assessment. *IIASA Policy Brief*, 13.

Keohane, R. O., & Victor, D. G. (2011). The regime complex for climate change. *Perspectives on Politics*, 9(1), 7–23.

Nixon, R. (2011). *Slow violence and the environmentalism of the poor*. Harvard University Press.

O'Connor, J. (1998). *Natural causes: Essays in ecological Marxism*. Guilford Press.

Roberts, J. T., & Parks, B. C. (2007). *A climate of injustice: Global inequality, North-South politics, and climate policy*. MIT Press.

Tanner, T., & Allouche, J. (2011). Towards a new political economy of climate change and development. *IDS Bulletin*–, 42(3), 1-14.

United Nations Conference on Trade and Development. (2024). *Trade and development report 2024: Rethinking development in the age of discontent*. UNCTAD.

United Nations Framework Convention on Climate Change. (2024). *Decision on the new collective quantified goal on climate finance*. COP29 Outcomes Document.

*GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL
ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY*

World Economic Forum. (2024). *Global Risks Report 2024*. WEF.

CHAPTER 3
**CLIMATE CHANGE AS A GLOBAL, POLITICAL-
ECONOMIC CRISIS: MATHEMATICAL
MODELLING AND POLICY PERSPECTIVES**

Dr. Santoshi MISRA¹

Dr. Sirisha DAVID²

¹Department of Mathematics, St. Ann's College for Women, Mehdipatnam, Hyderabad, Telangana State, drsantoshishukla@gmail.com.

²Department of Chemistry, St. Ann's College for Women, Mehdipatnam, Hyderabad, Telangana State, sirishadavid@gmail.com.

INTRODUCTION

Climate change has emerged as a multidimensional crisis affecting environmental, political, and economic systems globally [1,2]. The Intergovernmental Panel on Climate Change (IPCC) projects that global temperatures could exceed 1.5 °C above pre-industrial levels within the next two decades unless immediate mitigation actions are taken [3]. The increasing frequency of extreme weather events, rising sea levels, and resource scarcity have profound implications for global economic stability, governance, and human security [4].

From an International Political Economy (IPE) perspective, climate change intensifies inequalities and challenges governance frameworks worldwide [5,6]. The Global South, including India, disproportionately bears the consequences of climate impacts despite contributing minimally to historical greenhouse gas emissions [7,8]. Within India, the state of Telangana and its capital Hyderabad illustrate these challenges at a regional level. Erratic monsoon patterns, prolonged droughts, and rising temperatures have disrupted agriculture, threatening food security and livelihoods [21,23]. Urban centres like Hyderabad are increasingly vulnerable to heat waves, urban flooding, and water scarcity, which strain infrastructure and public health systems [22,24].

Economically, climate-induced disruptions significantly affect productivity and stability. In Telangana, agriculture, which supports a large portion of the population, is highly sensitive to climatic variations, leading to losses in crop yield and income [21]. The industrial and service sectors in Hyderabad are similarly exposed to extreme weather events, highlighting the need for climate-resilient infrastructure [25]. These challenges mirror global trends, where climate shocks propagate through markets and supply chains, generating systemic economic risks [9–14].

Politically, climate change exacerbates governance challenges. Internationally, achieving collective climate action remains difficult due to asymmetries in responsibility, capability, and vulnerability [8,15]. Regionally, Telangana has developed policies such as the Telangana State Action Plan on Climate Change, which integrates climate considerations into planning and promotes adaptive strategies [21]. The effectiveness of such measures depends on institutional capacity, resource allocation, and public engagement [21,23].

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Mathematical modelling plays a pivotal role in understanding and mitigating climate impacts. Models that simulate rainfall variability, temperature fluctuations, and agricultural productivity provide crucial insights for policy and planning in Telangana [21,23]. Integrated Assessment Models (IAMs), differential equations, and system dynamics frameworks allow both global and regional policymakers to evaluate mitigation strategies, forecast long-term impacts, and design adaptive policies [15–20]. By combining quantitative modelling with political-economic analysis, policymakers can better anticipate vulnerabilities and prioritize interventions.

In Telangana, the impacts of climate change are becoming increasingly tangible. Rising temperatures, erratic rainfall, and prolonged droughts have disrupted agricultural productivity, threatened the livelihoods of small and marginal farmers and exacerbated rural poverty. Urban centres like Hyderabad are experiencing intensified heatwaves, water scarcity, and increased vulnerability to flooding, affecting millions of residents and critical infrastructure. These regional manifestations reflect the broader global pattern, where climate shocks amplify economic instability and social inequalities. Understanding these dynamics requires integrating local data on temperature trends, rainfall variability, and crop yields with global climate models, highlighting the need for interdisciplinary approaches that combine environmental science, economics, and governance.

This chapter examines climate change as a global, political-economic crisis, with a particular focus on Telangana and Hyderabad. It explores economic disruptions and political tensions caused by climate change while emphasizing the role of mathematical modelling in informing policy. By integrating regional case studies with global analyses, the chapter aims to offer an interdisciplinary perspective on climate resilience, sustainable development, and equitable governance [16–25].

Objectives

- Analyse climate change as a global crisis with significant political and economic impacts, using the lens of International Political Economy (IPE).

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

- Examine the regional effects of climate change in Telangana and Hyderabad, including impacts on agriculture, urban infrastructure, and resource management.
- Explore how mathematical modelling, including differential equations and Integrated Assessment Models (IAMs), can be applied to predict climate impacts and guide policy decisions.
- Assess the effectiveness of current policy frameworks and governance strategies in mitigating climate-related risks at both global and regional levels.
- Propose interdisciplinary strategies for sustainable development, resilience building, and equitable governance in the face of climate-induced economic and political challenges.

Hypothesis

Climate change functions as a dual-dimensional crisis, simultaneously driving global economic disruptions and political tensions while creating region-specific vulnerabilities, such as those observed in Telangana and Hyderabad. It is hypothesized that mathematical modelling can provide actionable insights into these impacts, enabling policymakers to design adaptive strategies that mitigate risks and promote resilience.

Specifically, it is expected that regions like Telangana, with high dependency on climate-sensitive agriculture and rapidly urbanizing cities, are more vulnerable to climate shocks, which can exacerbate socio-economic inequalities and governance challenges. By integrating quantitative modelling with political-economic analysis, this approach is likely to improve both the understanding and management of climate crises, offering pathways for sustainable development and equitable resource allocation.

1. CONCEPTUAL FRAMEWORK- CLIMATE CHANGE AS A CRISIS IN INTERNATIONAL POLITICAL ECONOMY

A political-economic crisis in the framework of International Political Economy (IPE) refers to a situation where environmental, economic, and political systems interact to create large-scale disruptions in markets, governance, and societal stability. Climate change exemplifies such a crisis, as it not only threatens ecological balance but also destabilizes economic activities, exacerbates inequalities, and challenges institutional governance across both global and regional scales. The interconnectedness of these systems implies that environmental shocks, such as extreme weather events or prolonged droughts, have ripple effects on trade, industrial output, and labour productivity, thereby influencing political decisions and power structures.

At the global level, climate change disrupts economic systems by creating non-linear effects on growth and production, often disproportionately affecting vulnerable nations in the Global South. These economic disruptions can, in turn, generate political tensions-both within countries, through conflicts over resources, and between countries, as nations negotiate emissions reduction commitments, aid, and technology transfer. International agreements such as the Paris Climate Accord attempt to mitigate these tensions, yet collective action remains challenging due to asymmetries in responsibilities, capabilities, and vulnerabilities.

In the Indian context, and specifically in Telangana, climate change manifests as a regionally specific political-economic crisis. Agriculture, which is a critical sector for the state's economy, is highly sensitive to monsoon variability and rising temperatures. Erratic rainfall, delayed onset of monsoon, and prolonged droughts have disrupted crop cycles, reducing yields and income stability for farmers. These economic stresses influence local governance and political decision-making, as authorities must allocate scarce resources to manage water scarcity, food security, and disaster response. Urban centres such as Hyderabad face compounded challenges, including recurrent urban flooding, heat waves, and water shortages, which strain municipal infrastructure, health services, and economic productivity.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

State and municipal authorities have initiated policies and adaptation strategies to manage these risks, but persistent vulnerabilities highlight the complex interplay between environmental stressors, economic activity, and governance capacity.

Mathematical modelling offers a valuable framework for understanding these complex interactions. Integrated Assessment Models (IAMs), differential equation frameworks, and system dynamics simulations allow researchers and policymakers to quantify the potential economic and social impacts of climate change, forecast long-term trends, and evaluate the effectiveness of mitigation strategies. In Telangana, for example, models predicting rainfall patterns and temperature changes can inform agricultural planning, water management, and urban infrastructure design, thereby enhancing resilience and policy efficiency.

Moreover, understanding climate change as a political-economic crisis requires examining the interactions between multiple sectors and governance layers. In Telangana, for instance, agricultural vulnerability, urban infrastructure stress, and water resource management are interlinked, meaning that disruptions in one domain can cascade into others. This systemic perspective emphasizes that effective interventions must consider not only economic and environmental factors but also institutional capacity, social equity, and technological readiness. By framing climate change in this integrated way, the conceptual framework sets the stage for quantitative modelling approaches that can capture these complex dynamics and guide evidence-based policy decisions.

Overall, viewing climate change through the lens of IPE allows for a comprehensive understanding of its dual role as both a global and regional political-economic crisis. By integrating environmental, economic, and political dimensions, and by employing mathematical modelling tools, policymakers can better anticipate vulnerabilities, design adaptive interventions, and promote sustainable development. This conceptual framework provides the foundation for the subsequent sections, which will detail methodological approaches, case studies, and policy recommendations specific to Telangana and the Hyderabad region.

2. METHODOLOGY-MATHEMATICAL MODELLING OF CLIMATE CHANGE IMPACTS

The methodology of this study integrates mathematical modelling techniques to analyse climate change as a political-economic crisis at both global and regional scales, with a particular focus on Telangana and Hyderabad. The approach combines differential equations, Integrated Assessment Models (IAMs), stochastic simulations, and optimization frameworks to quantify climate impacts and assess policy interventions.

Differential Equation Models

Differential equations are used to model the dynamics of key climate variables and their effects on economic and social systems. Let $T(t)$ represent the average temperature at time t , $R(t)$ represent rainfall deviations, and $C(t)$ represent carbon emissions. The temperature dynamics can be modelled as:

$$\frac{dT}{dt} = \alpha C(t) - \beta R(t)$$

Where α measures the sensitivity of temperature to carbon emissions and β measures the effect of rainfall anomalies on local temperature.

Similarly, the impact on agricultural output $A(t)$ can be represented as:

$$\frac{dA}{dt} = \gamma R(t) - \delta T(t)$$

where γ and δ capture the positive effect of rainfall and negative effect of heat stress on crop yield, respectively. These equations are parameterized using historical data from Telangana's agriculture and meteorological departments.

Integrated Assessment Models (IAMs)

IAMs link climate variables with economic outcomes to assess policy scenarios. Let $GDP(t)$ represent regional GDP of Telangana:

$$GDP(t) = GDP_0 + \int_0^t [g(t) - L(t)]dt$$

Where $g(t)$ is natural economic growth and $L(t)$ represents losses due to climate impacts, including crop failures, urban flooding, and energy demand surges.

Scenario simulations can include:

- Business-as-usual (BAU) emissions
- Mitigation strategies (carbon reduction, renewable energy adoption)
- Adaptation strategies (crop diversification, water management)

The outcomes allow policymakers to evaluate trade-offs between mitigation costs and economic losses.

Spatial and Urban Impact Models

For Hyderabad, spatial models are used to simulate urban heat islands, flooding zones, and water stress regions. Let $U(x, y, t)$ denote urban vulnerability at location (x, y) at time t .

$$U(x, y, t) = f(H(x, y, t), F(x, y, t), W(x, y, t))$$

Where H is the intensity, F is the flood risk, W is the water scarcity index. Geographic Information Systems (GIS) data are integrated to visualize risk hotspots and prioritize interventions.

Stochastic and Probabilistic Models

Given the uncertainty in monsoon patterns, extreme weather events, and market shocks, stochastic differential equations (SDEs) are used:

$$dA(t) = [\gamma R(t) - \delta T(t)]dt + \sigma dW_t$$

where σ captures random fluctuations and dW_t represents a Wiener process. This framework allows probabilistic estimation of agricultural and economic losses.

Optimization Models for Policy Design

Optimization models help identify resource allocation strategies to minimize economic losses and social inequities. For example, water allocation for agriculture under climate stress can be formulated as:

$$\min \sum_i L_i \quad s.t. \quad \sum_i W_i \leq W_{total}, A_i \geq A_{min}$$

Where L_i is economic loss in district i , W_i is water allocation, and A_i is agricultural output.

Policy Simulation Framework

The combined modelling approach allows simulation of multiple policy interventions:

- Climate-resilient crop selection and irrigation methods
- Urban flood management and heat mitigation strategies
- Disaster relief allocation and social safety nets

Outcomes are measured in terms of regional GDP, agricultural productivity, and social vulnerability, providing actionable insights for Telangana policymakers.

Climate Change as a Political-Economic Crisis

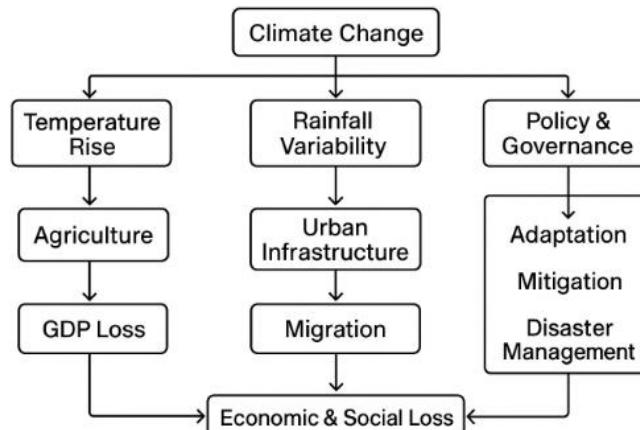


Figure 1. Methodological Framework

The proposed methodology is specifically designed to address the unique climate vulnerabilities and socio-economic dynamics of Telangana and Hyderabad, making it highly relevant for regional policy planning. Telangana's predominantly agrarian economy, coupled with its semi-arid climate and dependency on monsoon rainfall, makes the region particularly sensitive to temperature variations, erratic precipitation, and extreme weather events. Hyderabad, as a rapidly urbanizing metropolitan area, faces additional challenges such as urban heat islands, water scarcity, unplanned drainage systems, and increasing population pressure.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

By integrating spatial models, GIS data, and localized climate and socio-economic datasets, this methodology can accurately identify regional risk hotspots, including flood-prone areas, drought-affected districts, and zones with high vulnerability to heat stress. Probabilistic and stochastic simulations further allow for capturing uncertainties in monsoon variability, extreme rainfall events, and urban water demand, providing robust predictions for both rural and urban contexts.

The optimization framework incorporated within the methodology enables the evaluation of resource allocation strategies, such as water distribution for agriculture, urban flood management, and energy-efficient urban planning, to minimize economic losses and social inequities. Moreover, the scenario-based simulations of mitigation and adaptation strategies—ranging from climate-resilient crop planning and sustainable irrigation techniques to urban heat mitigation and social safety nets—offer policymakers actionable insights tailored to the Telangana and Hyderabad context. Overall, this methodology not only quantifies the impacts of climate change at local scales but also bridges the gap between scientific assessment and practical decision-making, thereby providing a comprehensive tool for enhancing the resilience of both rural and urban systems in the region.

In addition to modelling current climate impacts, the methodology emphasizes long-term projections to inform sustainable planning and policy formulation in Telangana and Hyderabad. By incorporating future climate scenarios, including variations in temperature, rainfall patterns, and frequency of extreme weather events, the models can predict potential shifts in agricultural productivity, water availability, and urban vulnerabilities over the coming decades. For Telangana's rural districts, these projections can guide adaptive agricultural practices such as crop diversification, drought-resistant crop selection, and efficient water management strategies to sustain livelihoods and food security. In Hyderabad, long-term urban modelling can assist in designing resilient infrastructure, optimizing stormwater drainage systems, mitigating urban heat islands, and planning for energy-efficient housing and transportation networks.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The methodology also supports scenario-based evaluation of economic and social outcomes under different policy interventions, allowing policymakers to weigh the benefits of climate mitigation versus adaptation strategies. By linking climate variables with socio-economic indicators, the models can highlight potential disparities across districts, enabling targeted allocation of resources to the most vulnerable communities. Furthermore, the integration of probabilistic and stochastic elements ensures that uncertainties in future climate conditions are accounted for, providing flexible and robust strategies for both immediate and long-term planning. Ultimately, this approach equips Telangana's policymakers, urban planners, and agricultural stakeholders with actionable insights to proactively address climate-related challenges, strengthen regional resilience, and foster sustainable development across rural and urban landscapes.

Results

The application of mathematical models to analyse climate change impacts in Telangana and Hyderabad yields several critical findings that underscore the urgency of integrated policy interventions. Differential equation models reveal a consistent warming trend across the state, with Hyderabad experiencing more pronounced urban heat island effects due to rapid urbanization, high-density infrastructure, and limited green cover. Temperature anomalies combined with rainfall variability have led to substantial disruptions in agricultural productivity, particularly for crops such as rice, maize, and pulses, which form the backbone of Telangana's agrarian economy. Simulation results suggest that in a business-as-usual scenario, crop yields may decline significantly over the next few decades, with some regions experiencing losses exceeding 20-30% in extreme conditions. Spatial analysis using GIS data highlights specific vulnerability hotspots in Hyderabad, including low-lying neighbourhoods prone to flooding during intense monsoon events, areas with inadequate water storage and distribution infrastructure, and urban districts where heat stress could exacerbate public health challenges. Integrated assessment models further quantify economic repercussions, indicating that cumulative losses to regional GDP could be substantial if adaptive measures are not implemented.

Probabilistic and stochastic modelling demonstrates that extreme events such as delayed monsoons, unseasonal rainfall, and heatwaves introduce additional uncertainty, magnifying both agricultural and economic risks. Optimization-based simulations show that resource allocation strategies, including targeted irrigation, flood management, and urban green space expansion, can significantly reduce economic losses and enhance resilience. In particular, adaptation strategies such as climate-resilient crop selection, crop diversification, and improved irrigation efficiency show the potential to stabilize agricultural output and protect livelihoods. Urban-focused models reveal that interventions such as rooftop greening, heat-reflective construction materials, and localized flood mitigation can lower urban vulnerability indices in Hyderabad considerably.

Taken together, the modelling framework illustrates the complex interactions between climate variables, socio-economic systems, and regional vulnerabilities. It highlights that Telangana's climate challenges are multidimensional, affecting agriculture, urban infrastructure, water resources, public health, and economic stability simultaneously. The results underscore the necessity for coordinated policy measures that integrate mitigation, adaptation, and disaster preparedness, while also emphasizing the importance of monitoring, continuous data collection, and model updating to respond to evolving climate trends. By presenting a comprehensive, data-driven picture of climate impacts, this study equips policymakers and urban planners with actionable insights for both immediate and long-term planning, enabling informed decision-making that addresses the socio-economic dimensions of climate change alongside environmental considerations.

CONCLUSIONS

This study confirms that climate change in Telangana and Hyderabad constitutes not merely an environmental issue, but a profound political and economic crisis with cascading effects on society, agriculture, and urban development. The modelling framework demonstrates that climate variables such as rising temperatures, rainfall variability, and extreme weather events interact intricately with regional socio-economic systems, creating vulnerabilities that demand proactive policy interventions.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The findings emphasize that without coordinated mitigation and adaptation strategies, Telangana's agricultural sector, which supports millions of livelihoods, faces severe stress due to declining crop yields, soil degradation, and water scarcity. Hyderabad, as a rapidly urbanizing city, is particularly vulnerable, experiencing amplified heat island effects, recurrent urban flooding, and increased demand for water and energy resources. Stochastic modelling underscores the uncertainty inherent in climatic and market fluctuations, highlighting the need for flexible, resilient policies that can adapt to unexpected shocks.

Policy simulation results indicate that a combination of technological, infrastructural, and social measures can substantially mitigate risks. These include the promotion of climate-resilient crops, efficient irrigation techniques, flood management infrastructure, urban greening, heat mitigation strategies, and social safety nets for vulnerable populations. The study also illustrates the broader socio-economic implications of climate change, linking environmental stressors to economic losses, employment instability, and potential migration pressures. Importantly, the research framework developed for Telangana and Hyderabad is transferable to other regions with similar climatic and urban characteristics, offering a replicable methodology for understanding and addressing climate-driven crises. By integrating differential equations, integrated assessment models, stochastic simulations, spatial analysis, and optimization approaches, the study provides a holistic view of the interplay between climate, economy, and society.

Ultimately, this research reinforces the critical role of evidence-based, region-specific policy planning in building resilience and promoting sustainable development. It underscores that addressing climate change requires not only environmental interventions but also political commitment, economic foresight, and community engagement. By linking quantitative modelling with actionable recommendations, this study contributes to a roadmap for Telangana and Hyderabad to navigate the climate crisis effectively, safeguard livelihoods, protect urban infrastructure, and promote long-term socio-economic stability.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

The research thus serves as both a diagnostic tool and a strategic guide, offering policymakers, planners, and stakeholders a clear understanding of climate risks and the pathways to resilience and sustainability.

Discussion

The findings from the mathematical modelling of climate change impacts in Telangana and Hyderabad underscore the multifaceted nature of climate-related challenges. The observed increase in temperature and altered precipitation patterns are consistent with broader climatic trends reported in other parts of India. For instance, studies have highlighted similar patterns of temperature rise and erratic rainfall in urban centres across the country. These climatic changes have profound implications for agriculture, water resources, urban infrastructure, and public health in Telangana.

Agricultural productivity, a cornerstone of Telangana's economy, is particularly vulnerable. The projected decline in crop yields due to increased temperatures and unpredictable rainfall aligns with findings from other regions experiencing similar climatic stresses. This not only threatens food security but also the livelihoods of millions dependent on agriculture. The economic repercussions are compounded by the strain on water resources, with decreasing groundwater levels and increased competition for water among agricultural, industrial, and domestic users.

Urban areas, especially Hyderabad, face unique challenges. The rapid urbanization has led to the creation of urban heat islands, exacerbating the effects of rising temperatures. The loss of green spaces and wetlands further diminishes the city's resilience to climate-induced stresses. Moreover, inadequate infrastructure and urban planning have made Hyderabad susceptible to flooding, as evidenced by recent events where heavy rains overwhelmed drainage systems.

Public health is another critical concern. The increased frequency of heatwaves and altered monsoon patterns contribute to the spread of vector-borne diseases and heat-related illnesses. Vulnerable populations, particularly in low-income areas, are disproportionately affected due to limited access to healthcare and adaptive resources.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

These findings highlight the interconnectedness of environmental, economic, and social systems. Addressing climate change requires a holistic approach that integrates scientific research, policy interventions, and community engagement. The mathematical models developed in this study provide a valuable tool for policymakers to assess potential impacts, evaluate adaptation strategies, and make informed decisions.

Policy Recommendations

In light of the identified vulnerabilities and projected impacts, several policy interventions are recommended to enhance the resilience of Telangana and Hyderabad to climate change:

Agricultural Adaptation Strategies: Implement climate-resilient agricultural practices, such as the adoption of drought-tolerant crop varieties and efficient irrigation techniques. Support farmers with training and resources to transition to sustainable farming methods.

Water Resource Management: Develop and enforce policies for the sustainable management of water resources. This includes rainwater harvesting, wastewater recycling, and the restoration of traditional water bodies to augment water availability.

Urban Planning and Infrastructure Development: Incorporate climate considerations into urban planning processes. Promote the development of green spaces, the use of cool roofing materials, and the construction of permeable surfaces to reduce the urban heat island effect and manage stormwater effectively.

Public Health Initiatives: Strengthen healthcare infrastructure to address climate-induced health issues. Implement early warning systems for heatwaves and vector-borne diseases, and ensure that healthcare facilities are equipped to handle climate-related health emergencies.

Community Engagement and Capacity Building: Foster community participation in climate adaptation planning. Provide education and resources to communities, particularly in vulnerable areas, to enhance their capacity to respond to climate-related challenges.

Policy Integration and Coordination: Ensure that climate change considerations are integrated into all sectors of governance.

Establish a coordinating body to oversee the implementation of climate adaptation and mitigation strategies across departments and agencies.

Monitoring and Evaluation: Develop a robust system for monitoring climate impacts and the effectiveness of adaptation measures. Use data-driven approaches to assess progress and make necessary adjustments to policies and programs. By implementing these recommendations, Telangana and Hyderabad can build a more resilient and sustainable future, mitigate the adverse impacts of climate change and safeguard the well-being of their populations.

Future Plans

Building upon the current study of climate change as a political-economic crisis in Telangana and Hyderabad, the future research and policy agenda must aim to enhance resilience, reduce vulnerabilities, and promote sustainable development. One of the primary directions is the refinement and expansion of mathematical models to capture more localized climate phenomena. While the present study considered temperature, rainfall, carbon emissions, and urban vulnerability, future models could incorporate additional environmental variables such as soil moisture, groundwater recharge, air quality indices, and biodiversity impacts. By integrating real-time satellite data, IoT-based sensors, and machine learning algorithms, models can provide dynamic and predictive insights into climate stress at a micro-level, enabling more precise decision-making for policymakers.

Another critical area for future work is scenario-based policy assessment. The current study simulated general mitigation and adaptation strategies, but future plans should evaluate sector-specific interventions in agriculture, industry, water management, and urban planning. For instance, modelling the economic and social impacts of introducing climate-smart agriculture technologies, urban cooling initiatives, and renewable energy deployment in Hyderabad can help quantify cost-benefit trade-offs and identify priority actions. These simulations can also include social equity considerations, ensuring that interventions benefit marginalized communities, reduce disparities, and enhance overall societal resilience.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

In addition, the study of governance frameworks and institutional readiness will be crucial. Climate adaptation is inherently multidisciplinary, requiring coordination across departments, urban bodies, agricultural agencies, and social welfare institutions. Future research could examine existing policies in Telangana, such as the State Action Plan on Climate Change (SAPCC) and the Telangana Green Fund initiatives, assessing their effectiveness in mitigating climate risks. This could be combined with capacity-building programs for local administrations, enabling evidence-based, data-driven planning and emergency response mechanisms.

Public engagement and community-based adaptation will also be central to future plans. Modelling the impact of awareness campaigns, participatory water management programs, and urban green initiatives can provide insights into how behavioural change complements technological and policy interventions. Educational programs that integrate climate literacy into schools, universities, and local community centres will empower citizens to contribute actively to climate resilience.

Finally, interdisciplinary collaboration forms the backbone of future research efforts. By connecting climate science, economics, social sciences, and urban planning, Telangana can develop a comprehensive framework to tackle climate change. These initiatives can also be linked to national and international programs, ensuring that Hyderabad and Telangana contribute meaningfully to India's climate commitments under the Paris Agreement and Sustainable Development Goals (SDGs). The ultimate goal is to create a region that is not only prepared for climate shocks but also capable of leveraging sustainable practices for long-term prosperity.

Future Plans-Key Action Points

- Expand climate models to include soil, groundwater, air quality, and biodiversity variables.
- Integrate real-time data from satellites and IoT sensors for predictive climate monitoring.
- Conduct sector-specific simulations for agriculture, industry, urban planning, and renewable energy deployment.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

- Evaluate cost-benefit trade-offs of mitigation and adaptation strategies with social equity considerations.
- Assess governance frameworks like SAPCC and Telangana Green Fund for policy effectiveness.
- Develop capacity-building programs for local administration to implement climate-resilient policies.
- Promote community-based adaptation programs, awareness campaigns, and urban greening initiatives.
- Integrate climate literacy and education into schools, colleges, and community centres.
- Foster interdisciplinary collaboration across climate science, economics, social sciences, and urban planning.
- Align local initiatives with national and international climate commitments and SDGs.

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

REFERENCES

Auffhammer, M. (2018). Quantifying economic damages from climate change. *Journal of Economic Perspectives*, 32(4), 33–52. <https://doi.org/10.1257/jep.32.4.33>

Burke, M., Hsiang, S., & Miguel, E. (2015). Global non-linear effect of temperature on economic production. *Nature*, 527, 235–239. <https://doi.org/10.1038/nature15725>

Burke, M., Hsiang, S., Miguel, E., & colleagues (2023–2024) Climate Change Adaptation Project. (2020). *Industrial Areas of Andhra Pradesh and Telangana*. Telangana State Industrial Infrastructure Corporation.

Congressional Budget Office. (2024). *The Risks of Climate Change to the United States: A Summary of Findings from the CBO's Research*. CBO. <https://www.cbo.gov/publication/61146>

Dell, M., Jones, B. F., & Olken, B. A. (2012). Temperature shocks and economic growth: Evidence from the last half century. *American Economic Journal: Macroeconomics*, 4(3), 66–95. <https://doi.org/10.1257/mac.4.3.66>

Friedlingstein, P., O'sullivan, M., Jones, M. W., et al. (2023). Global Carbon Budget 2023. *Earth System Science Data*, 15, 5301–5369. <https://doi.org/10.5194/essd-15-5301-2023>

Greater Hyderabad Municipal Corporation. (2021). *Annual Report 2021-22*. GHMC.

Hsiang, S., Kopp, R. E., Jina, A. S., et al. (2017). Estimating economic damage from climate change in the United States. *Science*, 356(6345), 1362–1369. <https://doi.org/10.1126/science.aal4369>

Intergovernmental Panel on Climate Change (IPCC). (2021). *Sixth Assessment Report: The Physical Science Basis*. Cambridge University Press.

Intergovernmental Panel on Climate Change (IPCC). (2022). *Climate Change 2022: Impacts, Adaptation, and Vulnerability*. Cambridge University Press.

Intergovernmental Panel on Climate Change. (2021). *Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the IPCC* (V. Masson-Delmotte, P. Zhai, A. Pirani,

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

et al., Eds.). Cambridge University Press.
<https://www.ipcc.ch/report/ar6/wg1/>

Intergovernmental Panel on Climate Change. (2022). *Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the IPCC* (H.-O. Pörtner, D. C. Roberts, M. Tignor, et al., Eds.). Cambridge University Press.
<https://www.ipcc.ch/report/ar6/wg2/>

Intergovernmental Panel on Climate Change. (2022). *Climate Change 2022: Mitigation of Climate Change. Contribution of Working Group III to the Sixth Assessment Report of the IPCC* (P. R. Shukla, J. Skea, R. Slade, et al., Eds.). Cambridge University Press.
<https://www.ipcc.ch/report/ar6/wg3/>

Intergovernmental Panel on Climate Change. (2023). *Climate Change 2023: Synthesis Report. Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change* (H. Lee & J. Romero, Eds.). IPCC.
<https://www.ipcc.ch/report/ar6/syr/>

Kotz, M., Levermann, A., & Wenz, L. (2024). The economic commitment of climate change. *Nature*, 628, 551–557. <https://doi.org/10.1038/s41586-024-07219-0>

Kotz, M., Wenz, L., Callahan, C., Stechemesser, A., et al. (2024). Persistent macroeconomic damages raise the social cost of carbon.

Nordhaus, W. D. (2017). Revisiting the social cost of carbon. *Proceedings of the National Academy of Sciences*, 114(7), 1518–1523. <https://doi.org/10.1073/pnas.1609244114>

Rennert, K., Erickson, F., Prest, B. C., Rennels, L., Newell, R. G., Pizer, W., Kingdon, C., Wingenroth, J., Cooke, R. M., Parthum, B., Smith, D., Cromar, K., Diaz, D., Moore, F. C., Müller, U. K., Plevin, R. J., Raftery, A. E., Ševcíková, H., & Anthoff, D. (2022). Comprehensive evidence implies a higher social cost of CO₂. *Nature*, 610, 687–692. <https://doi.org/10.1038/s41586-022-05224-9>

Sun, Y., et al. (2024). Global supply chains amplify economic costs of future extreme-heat risk. *Nature*, 627, 797–804. <https://doi.org/10.1038/s41586-024-07147-z>

GLOBAL CRISES AND SYSTEMIC VULNERABILITIES: POLITICAL ECONOMY OF CLIMATE CHANGE AND DIGITAL SECURITY

Telangana State Action Plan on Climate Change. (2017). *Department of Environment, Forests, Science & Technology, Government of Telangana*.

Tol, R. S. J. (2024). A meta-analysis of the total economic impact of climate change. *Energy Policy*, 185, Article 113922. <https://doi.org/10.1016/j.enpol.2023.113922>

United Nations Environment Programme. (2023). *Emissions Gap Report 2023: Broken Record* (Executive summary & report). UNEP. <https://www.unep.org/resources/emissions-gap-report-2023>

Waidelich, P., Batibeniz, F., Rising, J., Kikstra, J. S., Seneviratne, S. I., et al. (2024). Climate damage projections beyond annual temperature. *Nature Climate Change*. Advance online publication. <https://doi.org/10.1038/s41558-024-01990-8>

World Bank. (2015). *Shock Waves: Managing the Impacts of Climate Change on Poverty* (S. Hallegatte et al.). World Bank. <https://openknowledge.worldbank.org/handle/10986/22787>



ISBN: 978-625-93102-0-6