ABOUT THE BOOK

Beyond Firewalls: The Myth-Reality Divide in Cyber Security challenges the narrow view that cybersecurity is limited to tools like firewalls and antivirus software. It highlights how modern threats—such as phishing, ransomware, and social engineering—often exploit human vulnerabilities rather than technical flaws.

The book explores the "myth-reality divide" between perceived security and actual resilience. It argues that true cybersecurity depends on people, processes, and policies, not just technology.

Emerging risks like AI-driven attacks and cybercrime networks are also examined, especially in rapidly digitizing regions like India. Emphasizing strategies like Zero Trust, and continuous monitoring, the book advocates a proactive approach. Overall, it presents cybersecurity as an ongoing process requiring awareness, adaptability, and responsibility.

Editor-in-chief
Prof. (Dr.) Nirmal Kanti Chakrabarti
Prof. (Dr.) Paresh Kumar Acharya

Edited by:
Ms. Lamiya Sultana,
Dr. Chandrima Chakrraborty,
Ms. Ankita Mukherjee

9-78-81-993286-5-1

BEYOND FIREWALLS: 2026

SWAMI VIVEKANANDA UNIVERSITY
SVU

BEYOND FIREWALLS:

THE MYTH-REALITY DIVIDE IN CYBER SECURITY

Editor-in-chief
Prof. (Dr.) Nirmal Kanti Chakrabarti
Prof. (Dr.) Paresh Kumar Acharya

Edited by:
Ms. Lamiya Sultana,
Dr. Chandrima Chakrraborty,
Ms. Ankita Mukherjee

Edition: First Edition, 2025

Publisher: Swami Vivekananda University Press
Telinipara, Barasat–Barrackpore Road
Bara Kanthalia, West Bengal – 700121, India

Website: www.swamivivekanandauniversitypress.com

ISBN: 978-81-993286-3-1

BEYOND FIREWALLS

THE MYTH-REALITY DIVIDE IN CYBER SECURITY

SWAMI VIVEKANANDA UNIVERSITY

SCHOOL OF LEGAL STUDIES

EDITOR-IN-CHIEF

Prof.(Dr.) Nirmal Kanti Chakrabarti
Prof.(Dr.) Paresh Kumar Acharya

EDITED BY

Ms. Lamiya Sultana
Dr. Chandrima Chakraborty
Ms. Ankita Mukherjee

Swami Vivekananda University, Kolkata (Institutional Publisher) Published by the Swami Vivekananda University (Institutional Publisher), Kolkata-700121, West Bengal, India No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication. This edition can be exported from India only by the publisher. Swami Vivekananda University (Institutional Publisher), Kolkata-700121,

India. ISBN: 978-81-993286-3-1

First Edition: December,2025, Publisher: Swami Vivekananda University (Institutional Publisher), Kolkata700121,

India Contact: schooloflegalstudies@svu.ac.in

PREFACE

In an age where digital systems underpin nearly every aspect of human life, cybersecurity has emerged as both a shield and a paradox. *Beyond Firewalls: The Myth–Reality Divide in Cyber Security* is an attempt to navigate this paradox—where perception often diverges sharply from practice, and where confidence in protection can mask profound vulnerabilities.

The popular imagination tends to reduce cybersecurity to visible defenses: firewalls, antivirus software, and encryption tools. While these are important, they represent only a fraction of a far more complex ecosystem. This book challenges the comforting myth that technology alone can secure us. It argues instead that cybersecurity is as much about human behavior, institutional culture, governance structures, and evolving threat landscapes as it is about code and hardware.

Across its chapters, this work explores the gap between what individuals, organizations, and governments believe about cybersecurity and what actually unfolds in practice. Why do sophisticated systems still fail? How do human errors and cognitive biases undermine advanced defenses? Why do policy frameworks often lag behind technological change? These questions form the core of the inquiry.

This book is not written solely for technical experts. It seeks to engage students, policymakers, educators, and general readers who wish to understand cybersecurity beyond jargon and surface level narratives. By bridging theoretical insights with real-world examples, it aims to demystify complex concepts while encouraging critical reflection on widely held assumptions.

Importantly, *Beyond Firewalls* also emphasizes that cybersecurity is not merely a technical challenge but a societal one. Trust, accountability, ethics, and resilience are central themes that run throughout the discussion. In a world increasingly shaped by data and digital interdependence, security cannot be an afterthought—it must be an integrated and conscious practice.

This preface sets the stage for a journey that moves beyond simplistic binaries of safety and risk, strength and weakness, myth and reality. Instead, it invites readers to embrace nuance and complexity, recognizing that true cybersecurity lies not in absolute protection, but in continuous adaptation, awareness, and informed engagement.

Ultimately, this book hopes to inspire a shift in perspective—from seeing cybersecurity as a static barrier to understanding it as a dynamic, shared responsibility.

ACKNOWLEDGEMENT

We express our deepest gratitude to Swami Vivekananda University, Kolkata, India for its unwavering support and academic encouragement in the creation of *'Beyond Firewalls: The Myth-Reality Divide in Cyber Security'*. The University's steadfast commitment to academic excellence, interdisciplinary research, and social responsibility has provided a strong foundation for this scholarly endeavor. Its vision of nurturing critical inquiry and intellectual independence has played a pivotal role in shaping the direction and purpose of this work.

We are sincerely thankful for the intellectually stimulating environment fostered by the University, which enabled meaningful engagement with complex issues at the intersection of law and media. The emphasis placed on inclusive scholarship, ethical reflection, and academic freedom has significantly influenced the depth and perspective of the discussions presented in this volume.

Our heartfelt appreciation is extended to the School of Legal Studies for its continuous guidance, institutional support, and encouragement throughout the research and editorial process. The mentorship, collaborative spirit, and access to academic resources provided by the faculty and administration have been invaluable in bringing this collective scholarly effort to fruition.

We also express our sincere gratitude to all the contributors whose rigorous research, insightful analyses, and scholarly dedication have enriched this work. Their commitment to academic excellence has been instrumental in shaping the intellectual depth of the book. It is our earnest hope that *'Beyond Firewalls: The Myth-Reality Divide in Cyber Security'* will serve as a meaningful academic contribution, fostering critical dialogue on the relationship between cyber security and accountability.

CONTENTS

Chapter 1

Foundations of Cyber Security: Concepts, Definitions and Core Principles

Moumita De, State Aided College Teacher, Department of Human Rights, Ramakrishna Sarada Mission Vivekananda Vidyabhavan College and Ph.D. Research Scholar, Adamas University.

Abstract:

Cyber security is the discipline dedicated to protecting digital systems, networks, programs, and data from unauthorized access, misuse, disruption, or destruction. As societies increasingly rely on interconnected technologies, the need for structured security foundations has become critical. The foundations of cyber security are built upon clear concepts, precise definitions, and established core principles that guide protective measures across digital environments. Central to this field is the understanding of threats, vulnerabilities, risks, and controls, which together shape effective defense strategies. The Confidentiality, Integrity, and Availability (CIA) triad serves as a primary model, ensuring that information is accessible only to authorized users, remains accurate and unaltered, and is available when required. Additional principles such as authentication, authorization, accountability, and non-repudiation strengthen trust within systems. Risk management, governance frameworks, and security policies further support structured protection efforts. By integrating technical controls with organizational practices and human awareness, cyber security establishes a resilient defense posture. A strong foundation in these core concepts enables institutions and individuals to anticipate emerging threats, minimize potential damage, and maintain the reliability and stability of digital infrastructures in an evolving technological landscape.

Keywords: *Interconnected technologies, organizational practices and human awareness, cyber security.*

Introduction

In an era defined by digital transformation, cybersecurity has emerged as a central concern for governments, corporations, educational institutions, and individuals. The rapid expansion of internet connectivity and reliance on digital systems have created a landscape where cyber threats can inflict economic loss, privacy violations, reputational damage, and even national insecurity.

Cybersecurity, as a discipline, addresses the protection of systems and information from unauthorized access, damage, or disruption.[1]

[1] Clark DD and Landau S, *Cybersecurity: Toward an Interdisciplinary Approach* (Oxford University Press 2018).

Although the concept may seem simple, cybersecurity encompasses a complex array of technologies, processes, principles, and human behaviours. As such, a clear conceptual and definitional foundation is essential to understanding its practice and challenges. This paper synthesizes core ideas from academic literature, standards bodies, and industry frameworks to provide a comprehensive overview of the foundations of cybersecurity.

Core Concepts in Cybersecurity

Several foundational concepts underpin cybersecurity theory and practice. These concepts help structure understanding and guide implementation of security measures.

1. Confidentiality, Integrity and Availability (CIA Triad)

The CIA Triad remains the fundamental conceptual model in cybersecurity:

- Confidentiality: Ensures that sensitive information is accessed only by authorized entities. Mechanisms such as access controls, encryption, and authentication help enforce confidentiality.

- Integrity: Protects information from unauthorized modification, ensuring that data remains accurate and trustworthy. Hashing, digital signatures, and auditing are common integrity tools.

- Availability: Ensures that systems and information are accessible to authorized users when needed. Redundancy, fault tolerance, and disaster recovery strategies promote availability.[2]

Together, these three principles provide a foundation for evaluating and implementing security controls.

2. Authentication, Authorization and Accounting (AAA)

AAA is a model governing how user access is controlled:

- Authentication verifies the identity of a user or system component, typically through passwords, biometrics, or cryptographic keys.

- Authorization determines what an authenticated user is permitted to do.
- Accounting records actions performed by users, enabling auditing and accountability.[3]

AAA is central to access management in secure systems.

[2] Stallings W, *Effective Cybersecurity: A Guide to Using Best Practices and Standards* (Addison-Wesley 2017).

3. Defense in Depth

Defense in depth refers to the use of multiple, redundant security measures that protect a system at various level.[3] Rather than relying on a single control, a layered strategy increases resilience; if one control fails, others remain to mitigate risk.

Threat Landscape

Understanding threats is critical to designing effective cybersecurity measures. Threats vary in intent, sophistication, and impact.

Types of Threat Actors

Threat actors include:

- Malicious external actors: Cybercriminals, hacktivists, and state-sponsored groups who seek financial gain, political influence, or disruption.
- Insiders: Employees or contractors who intentionally or inadvertently compromise security.
- Automated threats: Bots and malware that operate without direct human control once released.[4]

Each actor type poses distinct challenges and requires tailored defences.

Common Attack Vectors

Some widely encountered attack vectors include:

- Malware: Software designed to disrupt, damage, or gain unauthorized access.
- Phishing: Social engineering attacks that deceive users into revealing credentials or executing harmful actions.
- Denial of Service (DoS): Attempts to overwhelm systems, making them unavailable to legitimate users. [3] Zwicky ED, Cooper S and Chapman DB, *Building Internet Firewalls* (O'Reilly Media 2000).
- Man-in-the-middle attacks: Intercepting communications between two parties to eavesdrop or manipulate data.
- Zero-day exploits: Attacks that exploit previously unknown vulnerabilities (Sutton, Greene & Amini, 2018).[5]

---

[3] Clark DD and Landau S, *Cybersecurity: Toward an Interdisciplinary Approach* (Oxford University Press 2018).
[4] Ibid.
[5] Casey E, *Digital Evidence and Computer Crime* (Academic Press 2011).

Principles of Cybersecurity

While foundational concepts explain what cybersecurity aims to protect, core principles describe how security should be structured and implemented.

1. Risk Management

Cybersecurity is fundamentally about managing risk. Risk is defined as the potential for loss when a threat exploits a vulnerability (ISO/IEC, 2018). A risk management approach involves:

- Risk identification: Cataloging assets, threats, and vulnerabilities.
- Risk assessment: Evaluating the likelihood and impact of potential events.
- Risk mitigation: Implementing controls to reduce risk to acceptable levels.
- Monitoring and review: Continuously assessing control effectiveness.

Frameworks such as NIST's Risk Management Framework provide structured approaches for organizations[6].

2. Security by Design and Default

Security by design means incorporating security principles into systems from the outset rather than as an afterthought. Systems should be built with robust defaults, minimizing insecure configurations and requiring explicit action to relax security controls.[7] This principle reduces the likelihood that systems are deployed with vulnerabilities.

3. Accountability and Auditing

Effective cybersecurity requires mechanisms to track and verify actions. Auditing and logging ensure that activities can be reviewed, investigated, and traced to responsible parties. These mechanisms support compliance and deter negligent or malicious behaviour.

4. Resilience and Recovery

Despite defences, breaches may occur. Resilience—the ability to maintain operations during and after an incident—is therefore crucial. Recovery planning includes backups, incident response teams, and continuity of operations plans. These capabilities reduce downtime and data loss.

---

[6] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (2021).

[7] Lipner S, *Security Design and Deployment in a Large Enterprise* (Microsoft Research 2005).

Security Controls and Technologies

A variety of security controls and technologies implement cybersecurity principles, ranging from technical tools to policy frameworks.

1. Cryptography

Cryptography protects data confidentiality and integrity through mathematical algorithms. Encryption transforms readable data into an unreadable format without a decryption key. Public key infrastructure (PKI) enables secure key exchange and digital signatures, which verify data origin and authenticity.[8]

2. Firewalls and Intrusion Detection Systems

Firewalls filter network traffic according to defined rules, preventing unauthorized access. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor for suspicious activity and can alert or respond automatically.[9]

3. Endpoint Protection

Endpoint protection tools secure devices such as laptops and mobile phones. Antivirus, antimalware, and endpoint detection and response (EDR) software detect, block, and remediate threats across user devices.[11]

4. Identity and Access Management (IAM)

IAM systems control how users authenticate and access resources. Features often include single sign-on, multi-factor authentication, and role-based access control, increasing both convenience and security.

Challenges and Future Directions

Cybersecurity continues to face evolving challenges.

1. Rapid Technological Change

Technological innovation—such as cloud computing, the Internet of Things (IoT), and automation—increases security complexity. These technologies expand attack surfaces and require new protective strategies.[10]

---

[8] Hadnagy C, *Social Engineering: The Science of Human Hacking* (Wiley 2018).

[9] Sutton M, Greene A and Amini P, *Fuzzing: Brute Force Vulnerability Discovery* (Addison-Wesley 2018). [11] Jaquith A, *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (Addison-Wesley 2007).

[10] Conti M, Dehghantanha A, Franke K and Watson S, 'Internet of Things Security and Forensics: Challenges and Opportunities' (2018) 78 *Future Generation Computer Systems*.

2. Skill Shortages

Demand for skilled cybersecurity professionals outpaces supply. Educational pathways, certifications, and workforce development efforts aim to address this gap but progress remains incremental.[11]

3. Global Collabouration

Cyber threats often cross-national boundaries, necessitating international cooperation. Agreements on norms of behaviour, information sharing, and joint response mechanisms enhance collective security

Foundational Dimensions of Cyber Security.

1. Governance and Strategic Alignment

Cybersecurity is not solely a technical function; it is a governance issue that must align with organizational strategy. Governance refers to the structures, policies, and decision-making processes that ensure cybersecurity objectives support broader institutional goals. According to Von Solms and Van Niekerk (2013), cybersecurity governance integrates risk management, compliance, and operational controls into executive-level oversight. Without strategic alignment, cybersecurity initiatives often become reactive rather than preventive.[12]

Board-level accountability has increasingly become essential. Senior leadership must define risk tolerance levels, allocate resources, and ensure regulatory compliance. The integration of cybersecurity into enterprise governance frameworks strengthens resilience and reduces fragmented security practices.[13]

2. Cybersecurity Frameworks and Standards

Foundational cybersecurity practices are often structured around recognized frameworks and standards. These frameworks provide systematic approaches to managing risk and implementing controls. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework organizes security activities into five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2021). This lifecycle approach reinforces that cybersecurity is continuous rather than static.[14]

Similarly, the ISO/IEC 27001 standard provides requirements for establishing, implementing, and maintaining an Information Security Management System (ISMS) (ISO/IEC, 2018). The ISMS model emphasizes continuous improvement through a "Plan–Do–Check–Act" cycle, promoting

---

[11] Ibid.
[12] Von Solms R and Van Niekerk J, 'From Information Security to Cyber Security' (2013) 38 *Computers & Security*.
[13] Ibid.
[14] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (2021).

adaptability to evolving threats.[15] These frameworks do not prescribe identical solutions but provide structured guidance adaptable to various industries and organizational sizes.

3. Cybersecurity Architecture and System Design

Secure architecture forms the structural backbone of cybersecurity. Security architecture refers to the design principles and models that define how security controls are integrated within systems. A well-designed architecture ensures that protection mechanisms are embedded into networks, applications, and data flows rather than added after vulnerabilities appear.[16]

One foundational architectural model is segmentation, which divides networks into smaller, isolated sections to limit the spread of attacks. Another is zero trust architecture, which assumes no user or device should be trusted automatically, even if inside the network perimeter (Rose et al., 2020). Under zero trust principles, continuous verification replaces implicit trust.[17]

Secure coding practices also contribute to strong architecture. Developers must anticipate misuse scenarios and design applications that minimize exploitable vulnerabilities. This proactive mindset aligns with the principle of security by design.

4. Incident Response and Digital Forensics

Even with strong preventive controls, security incidents are inevitable. Incident response is therefore a core cybersecurity function. An incident response plan outlines procedures for identifying, containing, eradicating, and recovering from cyber events.

According to Casey (2011), digital forensics plays a critical role in incident response by preserving and analysing digital evidence. Proper forensic procedures ensure that evidence remains admissible in legal proceedings and supports accurate root-cause analysis.[18] A structured incident response capability minimizes operational disruption, reduces financial loss, and strengthens future defensive strategies through lessons learned.

5. Cybersecurity Metrics and Performance Measurement

Measuring cybersecurity effectiveness remains a complex challenge. Unlike physical security, success in cybersecurity is often defined by the absence of incidents. However, quantitative and qualitative metrics can help organizations evaluate their posture.

---

[15] Ibid.

[16] International Organization for Standardization, *ISO/IEC 27000:2018 Information Security Management Systems — Overview and Vocabulary* (ISO 2018).

[17] Craigen D, Diakun-Thibault N and Purse R, 'Defining Cybersecurity' (2014) 4(10) *Technology Innovation Management Review*.

[18] Casey E, *Digital Evidence and Computer Crime* (Academic Press 2011).

Jaquith (2007) argues that meaningful security metrics should be consistent, inexpensive to gather, and aligned with business risk. Examples include mean time to detect (MTTD), mean time to respond (MTTR), patch management timelines, and user training completion rates.[19]

Metrics serve two primary purposes: demonstrating accountability and guiding improvement. Without measurement, organizations cannot determine whether security investments produce tangible benefits.

6. Supply Chain and Third-Party Risk

Modern organizations rely heavily on external vendors, cloud providers, and software suppliers. This interconnected ecosystem introduces supply chain risks, where vulnerabilities in third-party systems may expose core organizational assets. Boyson emphasizes that supply chain cybersecurity requires contractual controls, vendor risk assessments, and continuous monitoring. Organizations must evaluate third-party security maturity before integrating services or products into their environment.[20]

Recent high-profile breaches have demonstrated that attackers often exploit weaker suppliers to gain indirect access to larger targets. Therefore, cybersecurity foundations must extend beyond internal boundaries.[21]

Cybersecurity and Privacy Integration

Cybersecurity and privacy, while distinct, are deeply interconnected. Cybersecurity protects systems and data from unauthorized access, while privacy ensures that personal information is collected, processed, and stored responsibly.

Privacy-by-design principles require that data minimization, purpose limitation, and user consent mechanisms be integrated into system architecture. Strong cybersecurity safeguards support privacy compliance, but privacy governance also demands transparency and accountability in data usage practices.
Balancing operational needs with individual rights is a central ethical challenge in digital environments.

Ethical Hacking and Security Testing

Ethical hacking, also known as penetration testing, is a proactive strategy used to identify vulnerabilities before malicious actors exploit them. Security professionals simulate attacks under controlled conditions to evaluate system resilience. Penetration testing aligns with the principle of continuous improvement. By identifying weaknesses early, organizations can strengthen controls

---

[19] Jaquith A, *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (Addison-Wesley 2007).
[20] Sharma B and Sood SK, 'Fundamentals of Cybersecurity' (2020) 50 *Journal of Information Security and Applications*.
[21] Sandhu R and Samarati P, 'Access Control: Principles and Practice' (1994) *IEEE Communications Magazine*.

and reduce exposure. According to Allen (2012), structured testing methodologies improve both technical defences and organizational awareness. Ethical hacking reinforces the concept that security must be regularly evaluated rather than assumed effective.

Education and Capacity Building

Sustainable cybersecurity depends on education at multiple levels. Academic programs, professional certifications, and organizational training initiatives contribute to capacity building. Cybersecurity education must address technical competencies, legal awareness, and ethical reasoning.[22] National strategies increasingly emphasize workforce development to close the cybersecurity skills gap.[23] A well-trained workforce enhances both prevention and response capabilities. Education also extends to public awareness, empowering individuals to practice safe digital behaviour in everyday life.[24]

Conclusion

Cybersecurity is a multifaceted discipline rooted in protecting digital systems and data from unauthorized access, exploitation, and disruption. Its foundations rest on concepts such as confidentiality, integrity, and availability, and core principles including risk management, security by design, accountability, and resilience. Though grounded in technology, successful cybersecurity integrates human behaviour, organizational culture, legal compliance, and ethical practice.[25] As digital systems continue to evolve and intertwine with every aspect of modern life, the need for robust cybersecurity grows. A comprehensive foundation that blends theory, practice, governance, and awareness equips organizations and individuals to navigate an uncertain digital landscape with confidence and resilience. Expanding the foundation of cybersecurity requires moving beyond technical controls toward an integrated framework that includes governance, architecture, metrics, privacy, supply chain management, and workforce development. Cybersecurity is not a single technology or product but a structured discipline built upon risk management, strategic oversight, and continuous adaptation. As digital ecosystems become more complex, foundational principles must evolve to address interconnected systems, globalized threats, and regulatory expectations. A comprehensive understanding of these additional dimensions strengthens the theoretical and practical grounding of cybersecurity as an academic and professional field.

----------**********----------

[22] Craigen D, Diakun-Thibault N and Purse R, 'Defining Cybersecurity' (2014) 4(10) *Technology Innovation Management Review*.

[23] Von Solms R and Van Niekerk J, 'From Information Security to Cyber Security' (2013) 38 *Computers & Security*.

[24] International Organization for Standardization, *ISO/IEC 27000:2018 Information Security Management Systems — Overview and Vocabulary* (ISO 2018).

[25] Cavoukian A, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario 2011).

Chapter 2

Cybersecurity in the Digital Age—The Illusion of the Fortress

-Dr. Chandrima Chakraborty, Assistant Professor, School of Legal Studies, Swami Vivekananda University

Abstract

The traditional paradigm of cybersecurity, long characterized by the "fortress" metaphor, is undergoing a profound and necessary dissolution in the mid-2020s. For decades, organizational defense strategies were predicated on the existence of a clear digital perimeter—a "moat" of firewalls and encrypted gates designed to distinguish the trusted internal network from the untrusted external world. However, this abstract explores how the rapid acceleration of cloud ubiquity, the permanence of hybrid work, and the explosion of the Internet of Things (IoT) have rendered the perimeter obsolete. The "fortress" has become an illusion; when data is hyper-distributed across edge nodes and third-party providers, the walls no longer have a foundation upon which to stand.

This chapter examines the shift from static, perimeter-based defenses to the 'Zero Trust' architecture, which operates on the pragmatic assumption that a breach is either imminent or already in progress. In an era where AI-driven adversaries and state-sponsored actors can probe vulnerabilities at machine speed, the illusion of total exclusion has been replaced by a mandate for continuous verification. The research highlights that the greatest risk to modern digital infrastructure is not merely technical, but psychological: "breach fatigue" and a lingering reliance on the fortress mental model.

As we navigate 2026, the transition toward an "immune system" model of security—prioritizing detection, micro-segmentation, and rapid resilience over the futile hope of a permanent barrier—is no longer a choice but a survival requirement. This abstract concludes that true security in the digital age requires embracing the transparency of an open landscape, moving away from the hubris of the impenetrable wall and toward a culture of collective, identity-centric vigilance.

Keywords: *Zero Trust Architecture, Perimeter Dissolution, Digital Resilience, Identity-Centric Security, Cyber-Physical Convergence*

Introduction: The Architecture of a Paradox

The advent of the digital age heralded an era of unprecedented global connectivity, promising the democratization of information, the frictionless exchange of capital, and the dissolution of geographical boundaries. Central to this technological utopianism was the implicit promise that the digital infrastructure supporting modern society could be secured, managed, and controlled. Yet, as the digital estate has expanded, a profound paradox has emerged: the very technologies that empower modern society simultaneously engineer its deepest vulnerabilities. Cybersecurity, once

a niche discipline confined to the esoteric realms of computer science, has metastasized into a foundational pillar of national security, corporate governance, and individual civil liberties.[26]
This chapter situates cybersecurity within the conceptual framework of *Promise and Paradox: Myth, Reality and Public Perspectives*. It argues that public understanding and policy responses to cybersecurity are heavily influenced by enduring myths—chiefly, the "myth of the digital fortress" and the "myth of the sophisticated adversary."[27] These myths construct an artificial binary between absolute security and total vulnerability, obscuring the nuanced, asymmetric reality of the cyber threat landscape. By juxtaposing the public perspective against empirical realities and legal frameworks, this analysis reveals how the promise of a secure digital environment is continuously undermined by the paradox of hyper-connectivity. The chapter will traverse the historical evolution of cyber threats, deconstruct prevailing public myths, analyze the shifting paradigm of cyber law and regulation, and ultimately argue for a transition from an unattainable paradigm of absolute security to one of cyber resilience.

1. The Promise of the Connected World and the Genesis of Cyber Risk

To understand the contemporary paradox of cybersecurity, one must examine the genesis of the Internet. The nascent architecture of the Advanced Research Projects Agency Network (ARPANET) and the early Internet was fundamentally predicated on a philosophy of openness and trust. The engineers who designed the Transmission Control Protocol and Internet Protocol (TCP/IP) prioritized end-to-end connectivity and resilience over robust authentication or encryption. The promise was one of academic and governmental collabouration—a network that could survive localized node failures, but which inherently trusted the actors operating within it.[28] This "trust by design" was not a technical oversight but a functional requirement for a decentralized, experimental system. In the 1970s and 1980s, the community of users was small, homogenous, and bound by shared professional ethics. The threat model of the time focused on physical destruction or mechanical failure rather than malicious data exfiltration. Consequently, security was an afterthought—a peripheral layer that could be added later, rather than a foundational pillar of the architecture. This original sin of the Internet's design remains the bedrock upon which modern cyber risk is built.[29]

The Commercial Pivot and the Illusion of Safety

As the Internet transitioned from an academic enclave into the backbone of global commerce in the 1990s, the paradigm shifted. The commercialization of the web necessitated the secure transmission of sensitive data, leading to the development of protocols such as Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS). The "promise" evolved: the digital

---

[26] Ronald Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (McClelland & Stewart 2013) 45
[27] Janet Abbate, *Inventing the Internet* (MIT Press
[28] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic Books 2010) 198.
[29] Ibid.

economy assured users that through the deployment of encryption, firewalls, and antivirus software, their data and capital would remain inviolate.[30]

The 1990s represented a period of techno-optimism. The rise of the World Wide Web promised to democratize information, flatten corporate hierarchies, and create a "frictionless" global market. However, this frictionlessness was a double-edged sword. The same pathways that allowed a consumer in London to purchase goods from a vendor in Seattle also allowed a malicious actor in a third jurisdiction to probe the vendor's database for vulnerabilities. The introduction of SSL provided a "green padlock" of confidence, but it secured only the *conduit* of information, not the endpoints. This distinction was largely lost on the public, creating a false sense of security that persists today.

The Legal Genesis: Property vs. Packet

However, this technological promise birthed a corresponding legal and regulatory challenge. Early legislative attempts to govern cyberspace, such as the UK's Computer Misuse Act 1990, were reactive, designed to criminalize unauthorized access to computer material rather than to mandate proactive security architectures. The law treated the computer as property, equating digital intrusion to physical trespass. This property-centric view laid the groundwork for the first major public myth: the concept of cybersecurity as perimeter defense.[31]

By framing cyber-attacks as "trespass," the law implicitly suggested that if a company built a high enough "digital fence," it would be safe. This led to the "Castle-and-Moat" philosophy of IT security. Organizations invested heavily in firewalls to protect the internal network (the castle) from the external Internet (the wild). Yet, this model was fundamentally flawed for two reasons. First, it ignored the "insider threat"—the reality that an authorized user could be a malicious actor or a negligent one. Second, it failed to account for the inherent connectivity required by modern business, which necessitates "holes" in the firewall to allow for email, web traffic, and remote access.[32]

The Explosion of Connectivity: The IoT and Hyper-Expansion

The turn of the millennium brought the "Always-On" era. With the advent of broadband and later, the smartphone revolution, the boundary between being "online" and "offline" evaporated. The promise of the connected world expanded into the "Internet of Things" (IoT), where everything from industrial turbines to domestic refrigerators became a network node.

This hyper-connectivity exponentially increased the "attack surface."[33] In the early days of ARPANET, a security flaw might affect a handful of workstations. In the IoT era, a vulnerability in a common firmware component can compromise millions of devices simultaneously. The genesis of cyber risk thus shifted from the exploitation of individual computers to the exploitation of systemic dependencies. When we connected our critical infrastructure—power grids, water

---

[30] National Cyber Security Centre, 'Zero Trust Architecture design principles' (NCSC, 23 July 2021) https://www.ncsc.gov.uk/collection/zero-trust-architecture

[31] National Cyber Security Centre, 'Zero Trust Architecture design principles' (NCSC, 23 July 2021) https://www.ncsc.gov.uk/collection/zero-trust-architecture

[32] Ibid.

[33] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic Books 2010) 198.

treatment plants, and hospital systems—to the same protocols used for cat videos and social media, we inherited the vulnerabilities of the 1970s design within the essential services of the 21st century.

The Professionalization of Cybercrime

As the digital economy grew, so did the sophistication of its shadows. What began as "script kiddies" seeking notoriety evolved into a multi-billion-dollar shadow economy. The promise of the connected world—efficiency, speed, and anonymity—was perfectly mirrored by the criminal underworld.

Cybercrime became "as-a-Service" (CaaS). Today, a malicious actor does not need to be a coding genius; they can rent ransomware, purchase stolen credentials on the dark web, and hire "initial access brokers" to find a way into a target network. This commodification of risk means that the barrier to entry for high-impact attacks has plummeted, while the potential ROI for criminals has skyrocketed. The "Genesis of Risk" is no longer just a technical story; it is an economic one.[34]

The Geopolitical Dimension: Cyberspace as a Domain of Conflict

Parallel to the rise of criminal syndicates was the realization by nation-states that cyberspace provided a new, low-cost domain for espionage and sabotage. The promise of global collabouration was subverted by the reality of "Hybrid Warfare."

Governments began to view the Internet not just as a tool for communication, but as a strategic asset and a battlefield. The development of sophisticated state-sponsored tools, such as Stuxnet—designed to physically degrade Iranian nuclear centrifuges—marked a turning point. It proved that bits and bytes could cause kinetic, physical damage. This introduced a new layer of risk: the "collateral damage"[35] of state-on-state cyber activity, where malware designed for a specific target escapes into the wild, crippling global logistics or healthcare systems (as seen with the NotPetya and WannaCry outbreaks).

The Modern Paradox: Complexity as a Vulnerability

Today, we face a crisis of complexity. The modern enterprise environment is a patchwork of legacy systems, multi-cloud environments, third-party APIs, and remote workforces. Each layer of complexity adds a layer of risk. The "Promise" has become so integral to our survival that we cannot unplug, yet the "Risk" has become so systemic that we cannot fully secure it.

The myth of the "unhackable" system has been replaced by the philosophy of "Assume Breach." We have moved from trying to keep people out to trying to detect them once they are in. This shift reflects a maturing understanding of the genesis of risk: that in a world defined by connectivity, isolation is impossible.[36]

Reconciling the Promise and the Risk

The journey from ARPANET to the modern hyper-connected world is a story of incredible human achievement shadowed by inherent fragility. The promise of the connected world—limitless

---

[34] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic Books 2010) 198.
[35] Ronald Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (McClelland & Stewart 2013) 45
[36] Ibid.

information, global unity, and economic efficiency—is real, but it was built on a foundation of trust that no longer exists in a hostile digital environment.

The genesis of cyber risk was not a single event, but a gradual accumulation of technical debt, legal lag, and the inevitable dark side of human ingenuity. To move forward, we must stop treating cybersecurity as a technical "add-on" and start treating it as a fundamental requirement of a functional society. The future of the connected world depends not on building better walls, but on building more resilient systems that can withstand the inherent risks of the very connectivity that makes our modern lives possible. We must accept that the "Promise" and the "Risk" are two sides of the same digital coin—inseparable, and requiring constant, vigilant balance.

2. Deconstructing the Mythology of the Cyber Fortress

The public perspective on cybersecurity is deeply colored by heuristics and cultural narratives that fail to reflect the technical reality of modern networks. Central to this dissonance are two pervasive myths: the Myth of the Fortress and the Myth of the Hacker.

2.1 The Myth of the Fortress

For decades, the dominant metaphor for cybersecurity in both corporate strategy and public imagination has been the medieval fortress. In this paradigm, the organization or the individual sits securely behind a moat of firewalls, intrusion detection systems, and antivirus software. The objective is to keep the "bad actors" on the outside of the perimeter while allowing trusted actors to operate freely on the inside.

This myth is intrinsically flawed in an era of cloud computing, mobile devices, and the Internet of Things (IoT). The traditional perimeter has evaporated. Modern network architecture operates on a "de-perimeterized" basis, where data resides in distributed third-party servers, and employees access corporate networks from unsecured domestic routers. As the UK National Cyber Security Centre (NCSC) has articulated, reliance on perimeter defenses is insufficient to mitigate risks originating from complex supply chains and insider threats.[37]

Despite this technical reality, the public and many corporate boards continue to view cybersecurity as a binary state—one is either "secure" or "hacked." When a breach occurs, the public reaction often centers on a perceived failure of the fortress walls, rather than acknowledging that in a complex digital ecosystem, breach is an inevitability. The fortress myth breeds a dangerous complacency; it suggests that security is an end-state achievable through the procurement of the right technological appliances, rather than a continuous process of risk management.

2.2 The Myth of the Hacker

Complementing the myth of the fortress is the public mischaracterization of the adversary. Pop culture and media discourse frequently depict cybercriminals as hooded, solitary savants operating in dark basements, possessing quasi-magical abilities to bypass any technological defense. Alternatively, public discourse jumps to the opposite extreme, attributing every data breach to highly sophisticated, state-sponsored Advanced Persistent Threats (APTs).

---

[37] National Cyber Security Centre, 'Zero Trust Architecture design principles' (NCSC, 23 July 2021) https://www.ncsc.gov.uk/collection/zero-trust-architecture

The reality is starkly different and heavily commodified. The contemporary cyber threat landscape is dominated by the industrialization of cybercrime. The rise of Ransomware-as-a-Service (RaaS) models allows technically unsophisticated actors to rent sophisticated malware infrastructures, complete with customer support and payment processing interfaces.[38]

The paradox here is striking: while the public fears the omnipotent, algorithmic genius, the vast majority of cyber incidents exploit mundane, well-documented vulnerabilities. Unpatched software, misconfigured cloud storage buckets, and, most prominently, social engineering (such as phishing) remain the primary vectors of compromise. The 2015 breach of the UK telecommunications company TalkTalk serves as a prime example; despite generating significant public alarm regarding a sophisticated cyber-attack, the breach was executed by teenagers utilizing a basic, decades-old technique known as SQL injection.[39] The myth of the sophisticated hacker serves as a convenient scapegoat for organizations, allowing them to attribute breaches to an unpreventable "force majeure" rather than a failure of basic cyber hygiene.

3. The Reality: Asymmetry, Commodification, and the Human Element

Stripping away the myths reveals a reality defined by structural asymmetry. In cybersecurity, the defender must be successful 100 per cent of the time, monitoring an exponentially expanding attack surface. The attacker, conversely, only needs to be successful once.[40] This inherent asymmetry dictates that the cost of offense is continually decreasing, while the cost of defense is increasing exponentially.

3.1 The Internet of Things and the Expansion of the Attack Surface

The promise of the IoT is the seamless integration of physical objects with digital intelligence, resulting in "smart" homes, cities, and healthcare systems. However, the reality of IoT implementation is a security paradox. By embedding connectivity into historically "dumb" devices—from pacemakers to industrial control systems—society has exponentially expanded its attack surface.

Many IoT devices are manufactured with an emphasis on cost and time-to-market, leading to egregious security oversights, such as hardcoded default passwords and an inability to receive security patches.[41] The reality of this vulnerability was demonstrated by the Mirai botnet in 2016, which harnessed hundreds of thousands of compromised IoT devices (primarily webcams and routers) to launch massive Distributed Denial of Service (DDoS) attacks, temporarily crippling major portions of the global internet infrastructure.[42] Here, the public perspective often fails to recognize the systemic risk posed by individual consumer choices; an unpatched smart lightbulb in a private residence can be weaponized to undermine national digital infrastructure.

---

[38] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021* (Europol 2021) 14.

[39] Information Commissioner's Office, 'TalkTalk gets record £400,000 fine for failing to prevent October 2015 cyber attack' (ICO, 5 October 2016) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-cyber-attack/

[40] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (John Wiley & Sons 2004) 38.

[41] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd edn, John Wiley & Sons 2020) 612.

[42] Antonakakis et al, 'Understanding the Mirai Botnet' [2017] 26th USENIX Security Symposium 1093.

3.2 The Supply Chain Paradox

The reality of modern digital operations relies on vast, interconnected supply chains. Organizations do not write their own software from scratch; they utilize third-party libraries, cloud service providers, and managed service providers. This interdependence creates a paradigm where an organization is only as secure as its least secure vendor.

The SolarWinds supply chain attack, discovered in late 2020, exemplifies this reality. Suspected state-sponsored actors compromised the software build environment of SolarWinds, a company providing network monitoring tools to thousands of enterprises and government agencies globally. By inserting malicious code into legitimate software updates, the attackers bypassed the "fortresses" of the US Treasury, the Department of Commerce, and numerous Fortune 500 companies.[43] The public perception of securing one's own borders is rendered obsolete when the weapons are delivered through trusted, cryptographically signed updates.

3.3 The Human Element: The Weakest Link and the Strongest Asset

Perhaps the most significant disparity between myth and reality lies in the role of the human operator. While technological solutions attract the majority of capital investment, human psychology remains the primary target for attackers. Social engineering tactics, particularly phishing and spear-phishing, exploit human cognitive biases—trust, fear, urgency, and curiosity—to bypass technical controls.

Legally, this presents a significant challenge. The General Data Protection Regulation (GDPR) mandates that organizations implement "appropriate technical and organisational measures" to ensure data security.[44] However, courts and regulatory bodies struggle to define where technical responsibility ends and human culpability begins. In *WM Morrison Supermarkets plc v Various Claimants*, the UK Supreme Court had to grapple with the vicarious liability of an employer for the malicious, insider data breach committed by a disgruntled employee.[45] While the employer was ultimately found not vicariously liable, the case underscored the terrifying reality that no technical architecture can fully mitigate the risk of authorized users acting maliciously or negligently.

4. Public Perspectives: The Tension Between Privacy, Security, and Convenience

The public perspective on cybersecurity is characterized by a deep-seated cognitive dissonance. Surveys consistently show that individuals express high levels of anxiety regarding data privacy,

---

[43] FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor' (FireEye Threat Research, 13 December 2020) https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 32.

[45] *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12.

identity theft, and corporate surveillance.[46] The fallout from the Cambridge Analytica scandal demonstrated acute public outrage over the misuse of personal data.[47]

Yet, this expressed anxiety rarely translates into secure behavioral practices. This is the "privacy paradox": the divergence between individuals' stated concerns regarding their digital privacy and their actual behavior, which often involves freely trading personal data for access to "free" digital services.[48]

4.1 The Convenience-Security Trade-off

The reality of effective cybersecurity often introduces friction into the user experience. Multi-factor authentication (MFA), complex password policies, and data encryption require time and effort. The public, conditioned by the seamless, frictionless design of modern digital platforms, frequently views security measures not as protections, but as impediments.

This tension heavily influences corporate strategy and product design. Technology companies constantly balance the need to secure their platforms against the risk of user abandonment due to excessive security friction. Consequently, security is often "opt-in" rather than "secure-by-default," shifting the burden of risk management onto the consumer, who is typically ill-equipped to make informed technical decisions.

4.2 The Normalization of Breach

As cyber incidents have proliferated, a dangerous shift in public perspective has occurred: the normalization of the data breach. With millions of records exposed annually, individuals suffer from "breach fatigue." The public response to notification of a compromised password or stolen credit card data has transitioned from alarm to apathetic resignation. This apathy poses a significant challenge to regulators and policymakers. If the public accepts data breaches as the inevitable cost of participating in the digital economy, the political pressure on corporations to invest heavily in robust cybersecurity architectures diminishes.

5. The Legal and Regulatory Response: Chasing the Phantom

The law, by its nature, is backward-looking, reliant on precedent and established principles. Technology, conversely, is relentlessly forward-looking. This temporal disjunction has created a landscape where legal frameworks are perpetually struggling to regulate the reality of cyber threats. The law attempts to domesticate the wildness of cyberspace through the imposition of liability, regulatory standards, and international norms.

---

[46] Pew Research Center, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (Pew Research, 15 November 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[47] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 278.

[48] Susan Athey, Christian Catalini and Catherine Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' [2017] National Bureau of Economic Research Working Paper 23488.

5.1 From Property to Data Protection: The Evolution of Liability

Early jurisprudence struggled with the incorporeal nature of digital assets. English common law, for instance, historically held that information could not be stolen because it did not constitute "property" capable of being permanently deprived, as established in *Oxford v Moss*.[49] Consequently, legislative interventions were required to create bespoke offenses for cyber intrusions, such as the Computer Misuse Act 1990.[50]

However, the paradigm shifted significantly with the realization that the primary value in cyberspace is not the hardware, but the data it holds. The implementation of the GDPR across the European Union (and retained in UK law post-Brexit) represented a watershed moment in cybersecurity regulation. The GDPR fundamentally altered the corporate calculus of cyber risk by introducing the threat of astronomical fines—up to 4% of global annual turnover—for failures to secure personal data.[51]

The regulatory approach under Article 32 of the GDPR is principle-based, requiring a level of security "appropriate to the risk."[52] This avoids the pitfall of prescribing specific technologies that will inevitably become obsolete. Yet, it creates a reality where organizations are uncertain of their legal compliance until after a breach has occurred and a regulatory body, such as the Information Commissioner's Office (ICO) in the UK, conducts an ex-post facto assessment of their security posture.

5.2 The Limits of Civil Litigation

Parallel to regulatory enforcement, civil litigation regarding data breaches has expanded, though it remains legally complex. Plaintiffs frequently attempt to bring claims for distress resulting from a loss of control over their data following a cyber-attack. In *Lloyd v Google LLC*, the UK Supreme Court significantly curtailed the viability of "opt-out" class actions for data breaches under the Data Protection Act 1998, holding that claimants must prove actual material damage or significant distress, rather than mere "loss of control" of data, to secure compensation.[53]

This legal reality reinforces the paradox: while the public feels deeply violated by cyber breaches, the legal mechanisms for collective redress are strictly constrained. The law currently treats the exposure of personal data as an abstract harm unless quantifiable financial loss can be demonstrated, a standard that frequently leaves consumers without a remedy.

5.3 The International Paradox: Cyber Warfare and Sovereignty

The disparity between myth and reality is most acute in the realm of international law and state-sponsored cyber operations. The promise of the post-WWII international legal order was the prohibition of the use of force, enshrined in Article 2(4) of the UN Charter.[54] The paradox of the cyber age is that states can now inflict catastrophic damage on an adversary's economy, infrastructure, and democratic processes without ever crossing the threshold of an armed attack.

---

[49] *Oxford v Moss* (1979) 68 Cr App R 183.

[50] Computer Misuse Act 1990, s 1.

[51] General Data Protection Regulation, art 83(5).

[52] General Data Protection Regulation, art 83(5).

[53] *Lloyd v Google LLC* [2021] UKSC 50.

[54] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(4).

State-sponsored operations, such as the Stuxnet worm—which degraded Iran's nuclear enrichment centrifuges—or the NotPetya malware—which, while purportedly targeting Ukraine, caused billions of dollars in collateral damage globally—operate in a legal gray zone.[55] The attribution of cyber-attacks is notoriously difficult. Sophisticated actors utilize proxy servers, false flags, and commercially available malware to obscure their origins.

The *Tallinn Manual*, a comprehensive academic study by international legal scholars, attempts to apply existing international law to cyberspace.[56] However, it is not a binding treaty. The reality is that there is no comprehensive international consensus on what constitutes a cyber "act of war," nor are there universally accepted norms governing state behavior in cyberspace. States exploit this ambiguity, engaging in a perpetual, low-intensity conflict that falls just below the threshold that would trigger a conventional military response. The public perspective, often shaped by sensationalist headlines about "cyber pearl harbors," misunderstands this reality; cyber conflict is rarely about sudden, catastrophic destruction, but rather persistent espionage, economic subversion, and cognitive manipulation.

6. Zero Trust and Cyber Resilience: Reconciling Myth and Reality

Given the failure of the "fortress" model and the inherent asymmetries of the threat landscape, the cybersecurity industry and regulatory bodies are slowly transitioning toward a new paradigm: "Zero Trust" and Cyber Resilience.

6.1 The Zero Trust Architecture

Zero Trust is a fundamental departure from the fortress myth. It operates on the principle of "never trust, always verify."[57] In a Zero Trust architecture, no entity—whether inside or outside the network perimeter—is trusted by default. Access to data and resources is granted on a strictly least-privilege basis, requiring continuous authentication and authorization based on multiple data points, including user identity, device health, and geographic location.

This shift represents an alignment of technological architecture with empirical reality. It acknowledges that perimeters will be breached and that internal networks are inherently hostile environments. By micro-segmenting networks and encrypting data both at rest and in transit, Zero Trust seeks to limit the "blast radius" of a successful intrusion.

6.2 From Cybersecurity to Cyber Resilience

Simultaneously, policy is shifting from a focus purely on *security* (preventing the breach) to *resilience* (the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems).

---

[55] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown 2014) 350.

[56] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

[57] John Kindervag, 'Build Security Into Your Network's DNA: The Zero Trust Network Architecture' (Forrester Research, 5 November 2010).

The European Union's Network and Information Security Directive (NIS2), which entered into force in 2023, exemplifies this approach.[58] NIS2 expands the scope of regulated entities to include "essential" and "important" sectors, mandating not just preventive technical measures, but robust incident response, business continuity planning, and supply chain security assessments.

The legal mandate for resilience acknowledges the public paradox: we rely on digital systems for societal functioning, yet those systems are inherently fragile. Resilience accepts the inevitability of the cyber incident and focuses on ensuring that the delivery of critical services—water, electricity, healthcare, finance—can continue even while systems are under active compromise.

7. The Future Public Perspective: Education, Regulation, and Duty of Care

If society is to reconcile the promise of digital technology with the paradox of its inherent risks, a profound shift in public perspective and legal frameworks is required.

First, the narrative must change. Governments and corporations must cease peddling the myth of absolute security. Public communication regarding cyber risk must mature, treating cybersecurity not as a dark art practiced by hackers, but as a standard metric of public health and safety, akin to sanitation or road safety.

Second, the legal burden must shift from the end-user to the manufacturer. Currently, the software industry operates under a unique liability shield; End User License Agreements (EULAs) routinely disclaim all liability for security defects in software. There is growing momentum, particularly in the United States and the EU, to establish a "duty of care" for software developers, holding them strictly liable for shipping products with known vulnerabilities or failing to adhere to secure-by-design principles.[59] The UK's Product Security and Telecommunications Infrastructure Act 2022 represents a crucial first step in this direction, mandating minimum security requirements for consumer smart devices, such as the prohibition of universal default passwords.[60]

Third, the insurance market must mature. Cyber insurance was initially promised as the panacea for mitigating financial risk from cyber-attacks. However, the reality of systemic risk—the potential for a single vulnerability in widely used software to trigger thousands of simultaneous claims—has led insurers to drastically increase premiums and introduce sweeping exclusions for state-sponsored attacks or acts of cyber war.[61] The public and corporate perspective must recognize that insurance is a mechanism for transferring risk, not mitigating it, and it cannot replace robust internal resilience.

Conclusion: The New Reality of the Digital Frontier

The discourse surrounding cybersecurity is inextricably bound within the dichotomy of promise and paradox. The promise of an interconnected, frictionless digital utopia has been met with the

---

[58] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) [2022] OJ L333/80.

[59] Cybersecurity and Infrastructure Security Agency (CISA), 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default' (CISA, April 2023)

[60] Product Security and Telecommunications Infrastructure Act 2022, Part 1.

[61] Lloyd's Market Association, 'Cyber War and Cyber Operation Exclusion Clauses' (LMA Bulletin LMA21-042-PD, 25 November 2021).

harsh reality of an asymmetric, highly commodified threat landscape that exploits both technical flaws and human fallibility.

The public perspective has been distorted by the enduring myths of the impregnable digital fortress and the omnipotent hacker, leading to alternating states of unreasonable expectation and apathetic resignation. Legal and regulatory frameworks have historically struggled to keep pace, retrofitting outdated property laws onto digital assets and struggling to enforce borders in a borderless domain.

However, a shift is occurring. The technical transition towards Zero Trust architectures and the regulatory emphasis on cyber resilience represent a maturation of the field. They signify an abandonment of the myth of absolute security in favor of the realistic management of chronic risk.

Ultimately, resolving the paradox requires a holistic approach. It demands that the law imposes stricter duties of care on those who design the digital infrastructure; that organizations prioritize resilience over mere compliance; and that the public perspective evolves to understand that in the digital age, security is not a product to be purchased, but a continuous, shared responsibility. Only by dismantling the myths that obscure the realities of cyber threats can society secure the foundational promise of the digital revolution.

The metaphor of the "fortress" has long dominated our collective understanding of cybersecurity. We envisioned high walls of code, deep moats of encryption, and iron gates of firewalls designed to keep the "barbarians" at bay. However, as we navigate the complexities of the mid-2020s, it has become strikingly clear that this architectural approach is an outdated relic of a simpler time. In the digital age, the fortress is not just under siege; the very idea of a static, impenetrable perimeter is an illusion.

The Erosion of the Perimeter

The primary reason the fortress model failed is the disappearance of the "inside." In the early days of computing, data lived on localized servers, and users accessed it from physical offices. Today, the cloud has decentralized our data, and the Internet of Things (IoT) has extended the attack surface to our refrigerators, medical devices, and industrial sensors.

When the "walls" of your organization are spread across thousands of remote home offices and third-party cloud providers, the traditional perimeter ceases to exist. This shift has forced a move toward 'Zero Trust Architecture', a philosophy grounded in the mantra: 'Never trust, always verify.'

The Human Element: The Structural Flaw

No matter how reinforced the digital masonry, the human element remains the most unpredictable variable. Social engineering—phishing, pretexting, and deepfake impersonations—targets the person behind the keyboard rather than the software in the machine.

We have learned that cybersecurity is as much a psychological challenge as a technical one. A billion-dollar defense system can be bypassed by a single employee clicking a "Reset Password" link in a convincingly crafted email. Recognizing that humans are part of the system, rather than just users of it, is essential for moving beyond the illusion of a self-sustaining fortress.

From Defense to Resilience

Perhaps the most significant shift in our modern understanding is the acceptance of 'inevitability', The goal of cybersecurity is no longer the total prevention of intrusion—a goal that has proven impossible—but rather cyber resilience.

If the fortress is destined to be breached, the focus must shift to:

- **Detection**: How quickly can we spot the intruder?
- **Containment**: How do we prevent the breach from spreading to the entire kingdom?
- **Recovery**: How fast can we restore essential services?

Modern security emphasizes the "Mean Time to Detect" (MTTD) and "Mean Time to Respond" (MTTR). In this context, success is measured not by the absence of attacks, but by the grace and speed with which an organization survives them.

The Role of Artificial Intelligence

As we look toward the future, the arms race has moved into the realm of automation. We are now seeing the rise of 'AI-driven threats', where malware can adapt its behavior in real-time to avoid detection. Conversely, defenders are using machine learning to identify patterns of behavior that human analysts might miss.

However, we must be cautious. AI is not a "magic shield" that restores the fortress. It is a dual-use tool that increases the velocity of conflict. The digital age demands that we view security not as a product we buy, but as a continuous, evolving process of adaptation.

Feature	**The Fortress Illusion (Traditional)**	**The Modern Reality (Adaptive)**
Focus	Prevention and Perimeter	Detection, Response, and Resilience
Trust Model	Binary (Inside = Safe, Outside = Bad)	Zero Trust (Continuous Verification)
Primary Target	Software Vulnerabilities	Human Psychology & Supply Chains
Success Metric	Number of blocked attacks	Speed of recovery and containment

Final Thought

The "Illusion of the Fortress" was a comforting dream, providing a sense of security in an increasingly connected world. But true safety in the digital age requires us to wake up. We must trade our heavy, static armours for the agility of a living organism—one that senses danger, learns from every encounter, and recovers stronger than before.

Cybersecurity is no longer a department or a set of tools; it is a fundamental cultural requirement of modern life. We must build systems that are secure by design, users who are skeptical by nature, and organizations that are resilient by necessity. The walls are gone, but through vigilance and adaptability, we can still protect what matters most.

The concept of the “fortress” has long served as the primary metaphor for cybersecurity. In the early days of the internet, the digital world was envisioned as a collection of walled cities, where heavy perimeters, firewalls, and encrypted gates kept the barbarians at bay. We operated under the assumption that if we could simply build the walls high enough and make the moats deep enough, the data within would remain sacrosanct. However, as we navigate the complexities of the mid-2020s, it has become increasingly evident that this fortress is an illusion. The traditional perimeter has not just been breached; it has dissolved entirely. The digital age has ushered in a level of connectivity and architectural fluidity that renders the old defensive models obsolete, forcing a profound philosophical shift in how we perceive safety, privacy, and the very nature of trust in a hyper-connected world.

The primary driver of this dissolution is the sheer ubiquity of the cloud and the decentralization of work. In the modern landscape, data no longer lives in a central server room located in a physical basement. It is dispersed across a global web of third-party providers, edge computing nodes, and personal devices. When the “assets” are everywhere, the “walls” are nowhere. The illusion of the fortress relied on a clear distinction between the “inside” (trusted) and the “outside” (untrusted). Today, that distinction is a relic of the past. The rise of Remote-everything and the Internet of Things has turned every toaster, every wearable medical device, and every home router into a potential entry point for sophisticated actors. This interconnectedness means that a vulnerability in a seemingly insignificant piece of software on a sub-contractor’s laptop can lead to the systemic collapse of a multinational corporation. The fortress didn’t fall because of a frontal assault; it evaporated because the architecture it was meant to protect changed into something boundaryless.

Furthermore, the nature of the adversary has evolved beyond the capacity of static defenses. We are no longer merely defending against the lone “hacker” in a basement; we are facing state-sponsored entities, highly organized criminal syndicates, and autonomous AI-driven systems that can probe for weaknesses at a scale and speed impossible for human defenders to match. These actors do not view a firewall as a wall, but as a temporary delay. They exploit the “human element,” which remains the most persistent crack in the masonry. Social engineering, deepfake technology, and sophisticated phishing campaigns prove that the most expensive security hardware in the world is useless if a user can be manipulated into handing over the keys. This reality highlights the core flaw of the fortress mentality: it focuses on technical barriers while ignoring the fluid, psychological, and social dimensions of digital interaction.

In response to the crumbling of the fortress, the industry has shifted toward the “Zero Trust” framework. This represents a fundamental move away from the idea of a secure perimeter to a model of continuous verification. In a Zero Trust world, the assumption is that the breach has already happened. No user, device, or application is trusted by default, regardless of their location or previous history. While this is a more realistic approach, it also signals the end of digital peace of mind. We have traded the comforting (if false) security of the fortress for a state of permanent, high-alert scrutiny. This shift reflects a broader societal realization that absolute security is a myth. The digital age demands that we stop asking how we can prevent all attacks and start asking how we can remain resilient in the face of inevitable compromise.

The psychological impact of this “illusion of the fortress” cannot be overstated. For decades, the public was sold the idea that encryption and passwords were bulletproof. As massive data breaches become a weekly occurrence, the resulting “breach fatigue” has led to a dangerous sense of fatalism. If the fortress is an illusion, many feel there is no point in trying to secure their digital

lives at all. This apathy is perhaps the greatest security risk of our time. To counter this, we must move toward a more transparent dialogue about risk. We must accept that the digital age is inherently volatile. Security is not a state one achieves but a continuous, exhausting process of adaptation. The fortress has been replaced by the immune system—a model that focuses on detection, rapid response, and the ability to function while under attack, rather than the futile hope of total exclusion.

The emergence of Generative AI and quantum computing adds another layer of complexity to this crumbling facade. As we move closer to the era of quantum supremacy, the very mathematical foundations of our current encryption models—the stones of our fortress—threaten to turn into sand. Meanwhile, AI is being used to automate the creation of malware that can mutate to avoid detection, essentially creating "living" threats that evolve in real-time. This technological arms race ensures that the walls can never be finished. The moment a stone is placed, the adversary has already developed a tool to bypass it. This constant state of flux reinforces the central theme of our current era: the only constant in cybersecurity is change, and the only true vulnerability is the belief that we are ever truly "safe."

Ultimately, the lesson of the digital age is that the fortress was always a psychological crutch rather than a technical reality. Our reliance on digital systems is now so absolute that there is no "offline" world to retreat to. Our identities, our economies, and our physical safety are now inextricably linked to a medium that is, by its very design, open and exploitable. Recognizing the illusion of the fortress is not an admission of defeat, but a necessary step toward maturity. It allows us to move away from the hubris of thinking we can control the digital environment and toward a more humble, agile, and realistic strategy of risk management.

As we look toward the future, the goal should not be to rebuild the fortress, but to foster a culture of digital literacy and collective responsibility. Security can no longer be the sole province of the IT department; it must be a core competency for every citizen of the digital world. We must build systems that are "secure by design," rather than trying to bolt security onto the outside of inherently broken structures. We must also demand greater accountability from the tech giants who manage our data, moving away from a model that prioritizes convenience and speed over the fundamental rights of privacy and safety.

In conclusion, the "Fortress" is a ghost. In the digital age, we live in a world of glass houses and open roads. The transition from the fortress model to a model of resilience and continuous verification is the defining challenge of our generation. By acknowledging that the walls are gone, we can finally focus on what matters: the integrity of the data, the privacy of the individual, and the stability of the global networks that now sustain human civilization. We must embrace the discomfort of the open digital landscape, trading the false security of the wall for the sharp, necessary vigilance of the survivor. The age of the fortress is over; the age of resilience has begun.

----------*----------

Chapter 3

From Threats to Trust: Securing the Digital World

Sonia Das, Assistant Professor, Department of Political Science, St. Xavier's College, Maharo, Dumka.

Abstract

This chapter reinvents cybersecurity roots by leaving the technical definitions and fixed protection models behind. It claims that the source of protection does not only reside in the technological safeguards but also in the socio-technical governance, institutional design, and human behaviour. Modern cyber threats are working in integrated digital ecosystems, whereby states, nongovernmental organisations and individuals are all sharing complementary responsibilities. The long-standing ideas of traditional principles of protecting confidentiality, integrity and availability are no longer applicable in such settings to describe protection building or maintenance.

The chapter establishes a critical framework that broadens the fundamental principles to encompass trust, accountability, adaptability, and resilience. Trust is discussed as a structural state which is formed by architecture, control, and social requirements. The analysis of accountability relates to the problem of attribution, legal responsibility, and the problem of governance gaps in transnational cyber activities. Adaptability is given as an active capacity that would allow institutions to move in response to uncertainty and swift changes in technology. The conceptualisation of resilience is the ability to withstand the attacks and in addition, absorb the disruption, recover effectively, and reshape systems to respond to changing risks.

The impact of the organisational culture, economic interests, and political interests on the process of security outcomes is also given attention. The chapter puts emphasis on the fact that systemic vulnerabilities and human factors frequently cause more vulnerabilities compared to individual technical vulnerabilities. It would offer a progressive concept of cybersecurity based on adaptive governance and inclusive digital ecosystems by applying the risk management theory, governance studies, and ethical analysis. This redefinition is in line with other contemporary academic debates that cybersecurity should be viewed as a socio-technical and institutional problem, as opposed to that of only a technological problem. The chapter thus adds to a polished theoretical base of the future research, policies, and strategies in the field of cybersecurity.

Keywords: *Organisational culture, economic interests, accountability, adaptability, and resilience.*

Introduction: Reframing the Roots of Protection

Cybersecurity should be perceived as a dynamic issue of governance, which will not be limited to purely technical control systems. The conventional cybersecurity strategies are centred on perimeter defence, firewalls and intrusion detection systems. Nonetheless, these methods are required, but inadequate due to the growing complexity of threats that are linked up, along with

the wider socio-economic environment in which digital systems are used in. Modern cyberattacks use not only technical vulnerabilities but also socio-technical, which is based on the organisational culture, human behaviour and operational decision-making. The constraints of a narrow technical model are noted by research, and it is found that the systems that cannot unify both social and organisational dynamics are still vulnerable despite the high level of technical protection[62].

This chapter provides the claim that a range of core tenets of cybersecurity needs to change by including governance, trust, accountability, and resilience into its rationale. Governance models construct security due to institutional structures, cross-sector co-operation and regulatory policy as opposed to being merely technology changes. Governance perspective is an acceptance that actors like states, private organisations, and individuals have shared (distributed) roles to secure digital ecosystems, particularly with the growing pattern of interdependence between infrastructures.[63]

Conceptual Reorientation of Cyber Security Foundations

From Technical Defence to Socio-Technical Governance

The history of cybersecurity has been a more profound change in isolated technical control systems to socio-technical models of governance that are aware of interdependencies between technology, organisations and society. The classical security models that are based on perimeter defences like firewalls and antivirus software were based on the premise that the source of risks was external to a well-delineated border. However, the current digital worlds are dynamic, networked and can be permeable, i.e. it misses external demarcation of threats, but may occur within the socio-technical systems themselves. Scholars allege that cybersecurity will have to be redefined to help in tackling this complexity by combining social, organisational, economic, and political factors with technical interventions.

---

[62] Ceur, Towards operationalizing cyber resilience - a socio-technical analytical framework (2026) Accessed on 6th March 2026: https://ceur-ws.org/Vol-4134/paper7.pdf

[63] Hoong, Yang, and Davar Rezania. "Navigating cybersecurity governance: the influence of opportunity structures in socio-technical transitions for small and medium enterprises." *Computers & Security* 142 (2024): 103852.

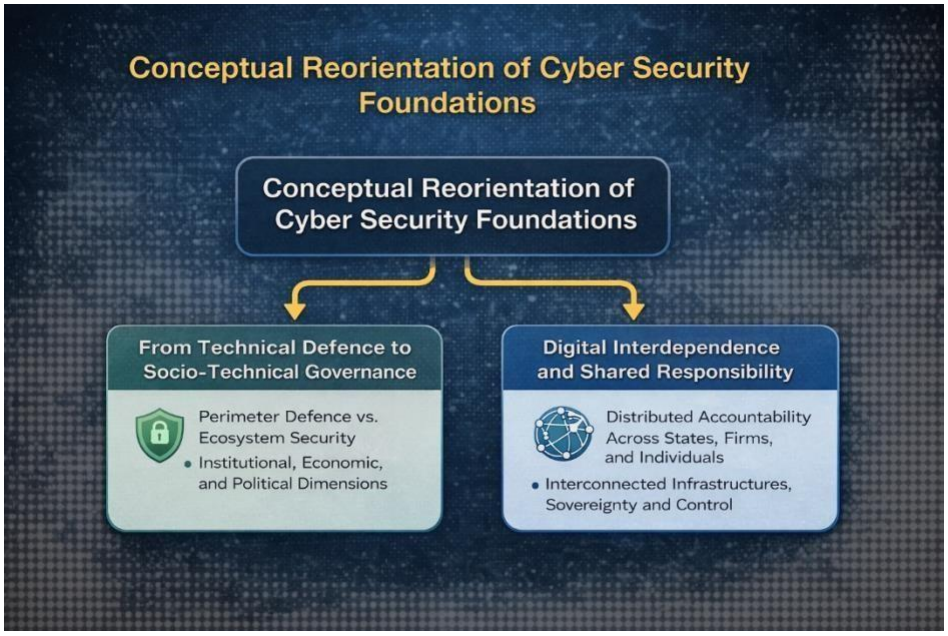


Figure 1: Cyber security conceptual reorientation

(Source: Self-Created)

A socio-technical system of governance is aware that technology and human actors share the same success in terms of security. Indicatively, cyber resilience models incorporate adaptive capabilities, including anticipation, recovery and learning in the system design with the focus placed on the cooptimisation of technical and human factors. This way of considering security is both as avoiding breaches and as the capacity to continue operation during periods of stress, a feature which in many old technical models is frequently ignored. In addition, the models of governance emphasise institutional and regulatory frameworks that affect the way organisations distribute resources, agenda-setting, and reaction to changing threats. Investing decisions and risk acceptance are influenced by institutional influences, economic factors and legal rules, i.e. cybersecurity efficiency is as much dependent on governance decisions as on technological initiatives.[64]

Adaptive governance also means that rulemaking and implementation of policies involve various stakeholders, such as the government, firms, and civil society[32]. This democratic governance is indicative of the fact of inter-relating digital ecosystems, where a failure in any part can spill over into widespread social or economic instabilities.[65]

[64] Ceur, Towards operationalizing cyber resilience - a socio-technical analytical framework (2026) Accessed on 6th March 2026: https://ceur-ws.org/Vol-4134/paper7.pdf

[65] Melaku, Henock Mulugeta. "A dynamic and adaptive cybersecurity governance framework." *Journal of Cybersecurity and Privacy* 3, no. 3 (2023): 327-350.

Digital Interdependence and Shared Responsibility

The concept of responsibility in cybersecurity goes further than the individual organisations to the networks of actors, as critical digital infrastructures are becoming more and more linked. Digital interdependence implies that a failure in one of the subsystems can be system-wide, so collective defence is necessary. Here, accountability is shared between the states, private businesses, and individual users.[66] Everyone has a contribution towards the process of establishing digital security and resilience. The research in cyberspace regulation confirms that the indefinite presence of security gaps exists because regulatory environments are disjointed and enforcement systems are inconsistent without integrated policy frameworks and multistakeholder interactions.

The notion of distributed accountability also transforms the conceptions of sovereignty and control in cyberspace. The conventional concept of national sovereignty presupposes territorial states and a central government. Conversely, infrastructures based on networks cross these boundaries, making it challenging to have state control and creating cooperative rules of governance.

Reconstructing Core Principles Beyond Traditional Models

Limits of Classical Security Principles

The classical concept of security that is based on the model of the static perimeter defence and deterministic control logics is becoming unsuitable in cloud-native, AI-enhanced, and platform ecosystem environments. The traditional "castle and moat" design presupposes definite borders and prescribed areas of trust, but digital space in the modern world has no boundaries. The cloud infrastructures are distributed across distributed services, microservices, and hybrid architecture, and there is a challenge to adhere to the static policies determined by network location.[67] The classical models rely on established rules and signatures that do not work with dynamic threats and new attack patterns that utilise AI-assisted exploitation and intra-service movement. Recurring vulnerability reporting and rule sets to older network arrangements will fail to keep up with the continuous integration and deployment, scale out, and on-demand resource provisioning found in cloud environments. Such incompatibility creates loopholes that are manipulated by advanced persistent threats to cause breaches that are not detected until a lot of damage has been done.

---

[66] Abrahams, Temitayo Oluwaseun, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu. "Cybersecurity awareness and education programs: a review of employee engagement and accountability." *Computer Science & IT Research Journal* 5, no. 1 (2024): 100-119.

[67] Qudus, Lawal. "Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges." *International Journal of Science and Research Archive* 14, no. 1 (2025): 1146-1163.

With AI-based systems, attackers can tamper with the models of learning or can feed the models with poisoned data as a tactic to avoid detection.[68]

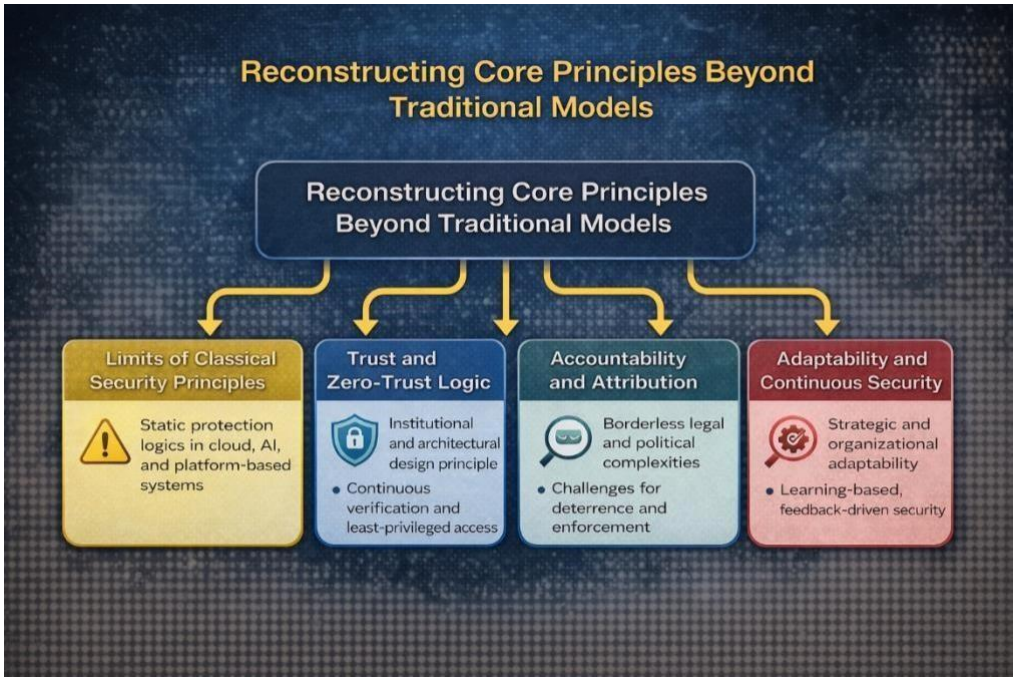


Figure 2: Reconstructing cybersecurity core principles

(Source: Self-Created)

Trust and Zero-Trust Logic as Governance Mechanisms

The implicit trust of traditional cybersecurity has been founded on the idea that users and devices within a perimeter are safe by default. By way of contrast, Zero Trust logic represents a principle of governance in which there is no automatic granting of trust but rather constant checking with respect to identity, context, and behaviour. Zero Trust philosophy, known as never trust, always verify, is becoming known as a strategic concept in the governance of security policies in digitally diverse environments, particularly in cloud and hybrid environments where former boundaries are melted away. Zero Trust must have continuous authentication of access, the least rights of access, and dynamic policy resolution of each access, irrespective of its source. This strategy changes the concept of trust not as a fixed quality but as an institutional and architectural design choice that is embedded in all the interactions. It drives organisations to the assumption that any element, user, or relationship can be hacked and implement policy choices that decrease implicit trust on the

[68] Anh, Nguyen Hoang. "Hybrid cloud migration strategies: balancing flexibility, security, and cost in a multicloud environment." *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems* 14, no. 10 (2024): 14-26.

network. In this manner, Zero Trust minimises attack points and limits the horizontal movement, which third-party traditional models tend to overlook, providing vast access once the initial perimeter defence is compromised.

Accountability and Attribution in a Borderless Environment

The concept of accountability in cybersecurity requires the ability to trace malicious practices back to a recognised actor, and this is difficult due to the borderless and obscured nature of cyberspace. Attribution, the process of identifying the origin of a particular cyber incident, is technically, legally, and politically difficult due to the use of anonymity, proxies, and the spread of infrastructure across the world.[69] The current cyber activities tend to cross borders, are nonstate activities and are proxies sponsored by states, and hence the lines of responsibility are blurred.

Adaptability and Continuous Security

Adaptability in cyber security focuses on strategic and organisational capability to adjust defence mechanisms to emerge threats. When the enemies keep on innovating, then the use of static controls becomes inadequate. Adaptive security is a dynamic control of policies driven by feedback, real-time observation and data analytics learnt by observing the behaviour of the system and threat information.[70] This model empowers systems to identify concept drift in patterns of threat and optimally retrain defensive mechanisms as environments evolve, ensuring that the detection accuracy remains and the resilience is maintained. Constant security is just a constant exposure to threats, constant presence of anomalies, and dynamism in policy implementation. There are examples of how learning-based frameworks can be more effective than just constant rule sets. Adaptive security conceptualises threats and defence as a coevolution process, where risk contextualised decision-making and intelligence integration across environments is a constant process.

Human Agency, Incentives and Systemic Vulnerability

Organisational Behaviour and Security Culture

Human behaviour in organisations is a core factor that determines the results of cybersecurity since it frequently influences the success or failure of these technical systems. Organisational culture implies a set of beliefs, values, and behaviours that affect the perception and relations of employees to cybersecurity policies and practices.[71] Empirical evidence indicates that when an organisation has a good security culture, meaning employee perception of security as part of their job and

---

[69] Gul, Seema, Wasmiya Malik, and Gohar Masood Qureshi. "Cybersecurity And Sovereignty: The Role Of International Law In Governing State Behaviour In Cyberspace." *Policy Journal of Social Science Review* 3, no. 5 (2025): 121-135.

[70] Farooq, M. and Khan, M.H., 2024. AI-driven network security: innovations in dynamic threat adaptation and time series analysis for proactive cyber defense. *Int. J. Wirel. Microwave Technol. (IJWMT)*, *14*(2), pp.17-26.

[71] Iyera, CA Vishwanathan, and Nilesh P. Gokhaleb. "Artificial Intelligence, Deepfakes, and Corporate Intelligence: A Systematic Literature Review on Ethical and Strategic Implications for Business Transparency and DecisionMaking." *Transforming Financial Management with AI, BI, and Data-Driven Decision Making* (2026): 67

mission, compliance is generated and behaviour risks associated with decision making biases or shortcuts are minimised. To illustrate, workers can disregard security controls by responding to them as heavyweight or not suitable to the productivity requirements, thus contributing to the heightening vulnerability. This is symptomatic of behavioural risk when convenience of preference or mental shortcuts are put ahead of security. Preparing resilience through such an investment in adaptive security awareness programmes and the integration of security norms into everyday actions makes secure behaviour a matter of practice instead of choice.[72]

Organisational security culture is strongly determined by leadership. Leaders with cyber security as their priorities instil a sophisticated environment whereby secure behaviour is acknowledged, justified, and aligned towards the business goals. On the other hand, leaders who consider cyber security an IT problem but not a strategic priority make employees have lax approaches to complying. Active leadership that sets expectations, incorporates security into the performance systems, and journalizes secure behaviour will contribute to increased risk awareness and a decrease in security fatigue, the level of exhaustion due to the continuous pressure to practise security that results in appropriation and slackness.[73] Human factors research points to the fact that security culture can never be elicited solely through policy, but it needs to be engaged, trained and reinforced with leadership and governance arrangements.

Cognitive biases that are associated with behavioural risks include overconfidence, routine behaviour and underestimation of threats. Such biases affect such decisions such as reusing passwords or disregarding suspicious warnings and reveal the weaknesses in the system.

---

[72] De Bruin, Marten, and Konstantinos Mersinas. "Individual and Contextual Variables of Cyber Security Behaviour-An empirical analysis of national culture, industry, organisation, and individual variables of (in) secure human behaviour." *arXiv preprint arXiv:2405.16215* (2024).

[73] Ibid.

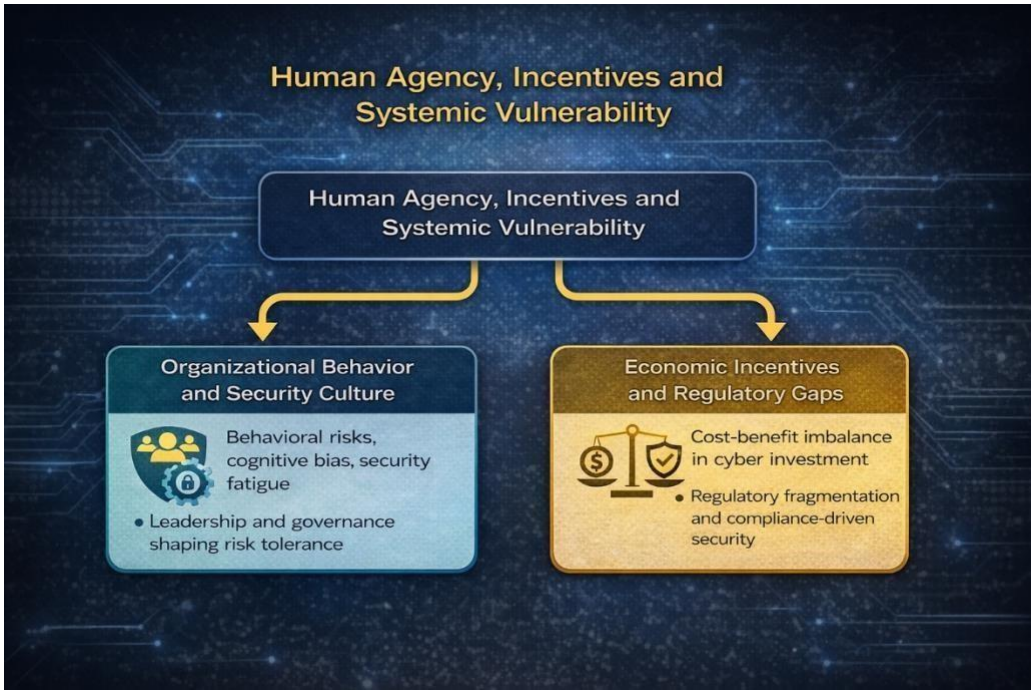


Figure 3: Human agency in cyber security dynamics
(Source: Self-Creaed)

Economic Incentives and Regulatory Gaps

Investments in cyber security are typically influenced by economic reasons and legislative conditions that may contribute to or create roadblocks in terms of organisational devotion to sound protective endeavours. The essence of the cost-benefit imbalance in the decision-making on cyber security lies in the fact that organisations consider the expense of security investments now and possible losses that are not present yet but might happen due to a breach. [74]

The regulatory frameworks affect the organisational behaviour to determine the incentives towards compliance and investment. Formulated regulations can influence risk management practises to improve through creating obligations towards incident reporting, risk assessments, and minimumsecurity standards. [75] Nonetheless, regulatory fragmentation through practice across jurisdictions and industries usually gives rise to unequal expectations and compliance costs, which are relatively more burdensome to smaller organisations. Disjointed regulatory systems may cause either duplication of needs or lack of enforcement, thus decreasing the overall efficiency of the policy incentives. Such mesquite may undermine group cyber resilience by enabling opponents to take advantage of jurisdictions that have looser enforcement.

[74] Farooq, M. and Khan, M.H., 2024. AI-driven network security: innovations in dynamic threat adaptation and time series analysis for proactive cyber defense. *Int. J. Wirel. Microwave Technol. (IJWMT)*, *14*(2), pp.17-26.
[75] Ibid.

Risk, Resilience and the Evolution of Protection Logic

Risk Management Under Uncertainty

Cyber security risk management commonly uses probabilistic models, estimating probability and the effects of threats, which are constrained in difficult digital systems (where uncertainty is common, interdependence is possible, and enemy behaviours are unpredictable). Conventional probabilistic models assume that previous data may be relied upon to forecast any form of risk, yet cyber threats change fast, and the previous trends cannot affect the study of the fresh attack vectors[46]. Additionally, the major variables like zero-day vulnerabilities, developing technology and human factors cause in-depth uncertainty that is a challenge to the statistical prediction and deterministic risk assumptions. Existing studies on cyber governance point to the fact that the risk management approach is usually deployed by organisations to regulate uncertainty but is potentially inadequate due to the tendency to view risk as a predictable aspect, as opposed to an outcome of socio-technical interactions.[76]

Complex digital environments have cascading failures and systemic risk, where a failure in some component of a network spreads to connected components and has an amplified impact compared to its original cause. Cascading failures. Unlike in non-networked systems, in a networked system, a failure in one component raises the risk of failure of a second component. The large-scale effects of risk are amplified in critical infrastructures like energy grids, finance, or supply chains, which initiates the small domino effect of isolated probabilistic models in that interdependency is not considered. The systemic risk arises not due to individual vulnerabilities but because of the collective behaviour of networked elements, and should be treated in a holistic manner, not in a fractured risk analysis manner.

Resilience as a Foundational Principle

Cyber resilience can be defined as the capacity of a system to receive, adapt to, and recuperate negatively affecting cyber events without disrupting vital operations and restoring operations rapidly. From a literary perspective, resilience is the ability to sustain critical activities in the presence of disruption and to reestablish the quality of the system after the event, thus resilience shifts the emphasis of prevention into an extended functionality in the face of stress environments (adaptive capacity). Companies that develop resilience as an organisational philosophy embrace pre-emptive threat detection, redundancy and recovery mechanisms that facilitate a rapid response and learning.[77]

---

[76] Iyera, CA Vishwanathan, and Nilesh P. Gokhaleb. "Artificial Intelligence, Deepfakes, and Corporate Intelligence: A Systematic Literature Review on Ethical and Strategic Implications for Business Transparency and Decision Making." *Transforming Financial Management with AI, BI, and Data-Driven Decision Making* (2026): 67

[77] Farooq, M. and Khan, M.H., 2024. AI-driven network security: innovations in dynamic threat adaptation and time series analysis for proactive cyber defense. *Int. J. Wirel. Microwave Technol. (IJWMT)*, *14*(2), pp.17-26.

Ethical and Strategic Foundations for the Future:

Security, Privacy and Civil Liberties

Growth in cybersecurity capabilities has led to a heightening confrontation between the national security interests and the safeguarding of privacy and civil liberties. An increase in defensive capacity is supported by surveillance technologies, data retention requirements, and algorithmic surveillance tools, though it raises the issue of proportionality and the rights of the individual. Unmonitored security operations are a threat to social confidence and democratic legitimacy.[78]

Transparency, Proportionality and Digital Solidarity

New ideas of cyber regulation in the future focus on transparency, proportionality, and digital solidarity. Exposure embodies effective communication concerning security practices, risks and accountability measures. Proportionality is used so that the protection measures are commensurate with the scope and characteristics of threats. Digital solidarity represents the shared digital security responsibility between involved states, the real actors, and civil society.[79] Governance structures that bring on board different stakeholders can empower legitimacy, propagate confidence, and equity in securing similar administration results in interdependent societies.

Conclusion: Re-Rooting Protection in Adaptive Governance

By considering socio-technical complexity that affects cybersecurity as an adaptive governance issue, this chapter has relegated the notion of technical control in efforts to resolve the issue. It has demonstrated that shared protection logics are not enough in the interconnected digital ecosystems. Enhanced general principles - trust, accountability, adaptability and resiliency, offer a stronger model of dealing with systemic risk and uncertainty. Both human behaviour and economic motivations, and regulatory frameworks have a great impact on vulnerability and response capacity.

---

[78] Farooq, M. and Khan, M.H., 2024. AI-driven network security: innovations in dynamic threat adaptation and time series analysis for proactive cyber defense. *Int. J. Wirel. Microwave Technol. (IJWMT)*, *14*(2), pp.17-26.
[79] Iyera, CA Vishwanathan, and Nilesh P. Gokhaleb. "Artificial Intelligence, Deepfakes, and Corporate Intelligence: A Systematic Literature Review on Ethical and Strategic Implications for Business Transparency and DecisionMaking." *Transforming Financial Management with AI, BI, and Data-Driven Decision Making* (2026): 67

Chapter 4

Gendered Cyber Insecurity: Between Legal Architecture and Lived Reality

Fazle Wakil, Research Scholar, Department of International Relations, Jadavpur University and

Anneshya Sanyal, Research Scholar, School of International Relations and Strategic Studies, Jadavpur University

Abstract

Cybersecurity, a foundation stone of the digital age, affects individuals across all demographics, yet its connection with gender is often unnoticed. The surge in importance of cybersecurity has not diminished the ever-present obstacles related to gender equality and the underrepresentation of women in this field. From online harassment to cyber-stalking, from cyber-bullying to hate speech, from threats to image-based abuse, from revenge pornography to discrimination, women and other marginalised genders experience heightened risk of cybersecurity. The gendered approach to cyber security is interconnected with the other aspects; complexities and needs of people based on gender, religion, race and sexual orientation. Gender-based violence is not a new phenomenon, but its migration to the digital world has magnified its scale and impact. The digital age has transformed how people interact, communicate, and conduct business. While the internet has provided numerous benefits, it has also given rise to new forms of crimes, particularly cybercrimes against women. These crimes not only invade the privacy of women but also threaten their safety, dignity, and mental well-being.

The rapid revolution in the IT industry, with a cornerstone of Artificial Intelligence, has affected the lives of individuals at large. People are more connected and engaged with each other on online platforms compared to physical interactions. These developments have assisted in some instances, but put privacy in danger. Women fear giving any of their details on any online platform due to the lack of security and privacy. Gender and cybersecurity are two correlated terms which have gained popularity in recent years. Privacy and security are still questioned in this era. Despite global progress and increased representation of women across various fields, this issue remains a major setback, limiting potential advancements in cybersecurity as a crucial societal factor. This imbalance deprives the field of talent and weakens its capacity to address new threats. In the field of cybersecurity specifically, according to figures from the International Information Systems Security Certification Consortium, that are based on a study carried out in 2019, women who work in cybersecurity represent only 24% of the total workforce globally.

Cybercrime against women has emerged as a critical concern within the United Nations system, particularly through the work of the International Telecommunication Union (ITU). Since its establishment in 1865, the ITU has addressed evolving technological risks from telegraphy to the internet age recognizing cybersecurity as foundational to a connected society. The proliferation of malware, cyber terrorism, and organized digital crime has intensified vulnerabilities,

disproportionately affecting women online. The rise of cybercrimes against women in India has also prompted the development of a multi-layered legal framework. The Information Technology Act, 2000 criminalizes hacking, identity theft, and electronic stalking, while enabling specialized cybercrime investigation cells. The Indian Penal Code has been amended to address voyeurism, cyberstalking, and non-consensual dissemination of intimate material. Additionally, the Protection of Women from Domestic Violence Act, 2005 extends protection to online harassment within abusive relationships. Although this framework is normatively robust, enforcement deficits, limited institutional capacity, and low awareness among women continue to constrain effective access to justice and meaningful digital protection.

Despite this layered statutory architecture, the paper argues that the gap between law on the books and law in action remains significant. The existence of multiple statutes and institutional mechanisms inevitably raises a critical question: have these legal interventions meaningfully reduced cybercrimes against women, or are such offences continuing to escalate in scale? The available trends suggest that reported cases are rising year after year which partly due to increased awareness and reporting, but also because digital dependence has deepened across every sphere of life. In an era where education, employment, governance, finance, and even intimate relationships are mediated through technological platforms, disengagement from digital systems is neither feasible nor desirable. This structural dependence renders women simultaneously visible, accessible, and vulnerable in unprecedented ways. Also while dealing against cybercrime as a whole, the inquiry must move beyond statutory adequacy to assess whether institutions possess technological capacity, trained personnel, and gender-sensitive protocols, while critically examining accountability when violations arise externally or within power structures, complicating the assumption of the state as an unequivocal protective actor.

This paper thus moves beyond formal legal analysis to examine patterns of incidence, enforcement capacity, infrastructural preparedness, and systemic accountability. By situating cybercrime within broader structures of digital governance and gendered power relations, it seeks to evaluate whether women's digital safety is substantively secured or remains an aspirational promise within an increasingly technologized society. Finally, the paper evaluates the effectiveness of existing cybersecurity frameworks themselves. Cybersecurity often operates reactively rather than preemptively, and rapid technological innovation frequently outpaces regulatory adaptation. The study therefore assesses whether current cybersecurity mechanisms function as meaningful deterrents or merely as post-facto response systems.

Keywords: *Privacy, Information Technology Act, Gendered Cyber Violence, Digital Governance, Institutional Capacity, Women's Online Safety, International Telecommunication Union*

Introduction – Gendering Cybersecurity

The expansion of the internet and digital technologies has fundamentally transformed the architecture of contemporary social life. Digital platforms now shape the way individuals communicate, access information, conduct economic activities, and participate in political and cultural processes. From education and governance to commerce and interpersonal interaction, the

digital sphere has become deeply embedded within everyday life. Within this rapidly evolving technological landscape, cybersecurity has emerged as a critical mechanism for safeguarding digital infrastructures and protecting individuals from malicious attacks, data breaches, and unauthorized access.[80] In its broadest sense, cybersecurity refers to the set of technological, legal, and institutional measures designed to protect computers, networks, servers, devices, and data from digital threats. However, while the digital revolution has generated unprecedented opportunities for connectivity and empowerment, it has also produced new vulnerabilities that affect users in unequal ways. The risks associated with cyber threats do not operate in a social vacuum. Instead, they intersect with existing structures of inequality embedded within societies. Among the groups most affected by these vulnerabilities are women, who frequently encounter disproportionate exposure to online harassment, privacy violations, and digital exploitation. Gender biases, patriarchal social norms, and structural inequalities often shape women's experiences in digital environments, making cybersecurity not only a technical issue but also a deeply social and political one.[81] As the digital domain increasingly functions as a site of social interaction, economic participation, and political expression, the absence of gender-sensitive cybersecurity frameworks raise important concerns regarding safety, equality, and access.

The relationship between gender and cybersecurity has therefore gained increasing scholarly and policy attention in recent years. Digital spaces often replicate and, at times, intensify existing social hierarchies. Women's participation in online environments is frequently shaped by cultural expectations, discriminatory attitudes, and institutional limitations that influence their access to technology as well as their ability to use it safely.[82] A gendered understanding of cybersecurity recognizes that digital threats are experienced differently across social groups. It draws attention to the ways in which vulnerabilities are influenced by intersecting identities such as gender, race, religion, sexual orientation, and socio-economic status. Consequently, addressing cybersecurity challenges requires a broader analytical lens that acknowledges how online harms disproportionately affect certain communities.[83]

Online harassment represents one of the most visible manifestations of gendered insecurity within digital environments. As digital communication platforms expand, they have simultaneously become spaces where abusive and discriminatory behaviour can proliferate with relative anonymity. The Dart Centre for Journalism and Trauma defines online harassment as any unwanted verbal or non-verbal behaviour that occurs in digital spaces and violates the dignity of an individual by creating a hostile, degrading, or offensive environment. This definition highlights the psychological and emotional consequences of cyber abuse, demonstrating that online harassment is not merely an inconvenience but a serious violation that can affect an individual's well-being, reputation, and sense of safety.[84] Women frequently encounter a range of abusive practices in online environments, including threats, trolling, hate speech, doxxing, cyberstalking, and other

---

[80] Wall DS, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007)
[81] Yar M and Steinmetz KF, *Cybercrime and Society* (3rd edn, Sage Publications 2019)
[82] Kshetri N, *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan 2013)
[83] Singer PW and Friedman A, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014)
[84] Ibid.

forms of targeted harassment. These practices are often rooted in misogynistic attitudes that seek to intimidate or silence women who participate in public discourse. Social media platforms, online forums, and digital communication channels have increasingly become arenas where gender-based hostility manifests through coordinated attacks and derogatory commentary. For many women, navigating digital spaces involves constant negotiation between the benefits of online participation and the risks of exposure to harassment.[85]

The broader context of cybercrime further underscores the significance of these challenges. Cybercrime has become a global phenomenon, affecting millions of individuals each year. Statistical estimates suggest that cybercrime occurs at an alarming frequency worldwide, with new victims emerging every few seconds. These figures illustrate the scale of the problem and highlight how deeply cyber risks have become embedded within modern societies. As the information technology sector continues to evolve particularly with the integration of artificial intelligence, machine learning, and data-driven algorithms the digital ecosystem has become increasingly complex.[86] Individuals now rely on digital platforms not only for communication but also for financial transactions, professional activities, and personal relationships. This rapid technological transformation has led to a paradoxical situation in which increased connectivity coexists with heightened vulnerability. While digital technologies enable individuals to build networks, share knowledge, and access opportunities, they also expose users to surveillance, data exploitation, and identity-related risks. Personal information shared online can be stored, analysed, and potentially misused by a range of actors, including corporations, governments, and cybercriminals. Privacy concerns have therefore become central to contemporary debates about digital governance and technological ethics.[87]

The tension between technological advancement and privacy protection has long been recognized. In 1999, Scott McNealy, the then Chief Executive Officer of Sun Microsystems, famously remarked that "privacy is dead—get over it." Although the remark was controversial, it reflected a growing recognition that digital technologies were fundamentally altering traditional notions of privacy. Over the past two decades, the proliferation of social media platforms, mobile applications, and data-driven services has intensified these concerns. The widespread collection and monetization of personal data have blurred the boundaries between public and private life, raising important questions about who controls digital information and how it is used. For women navigating digital spaces, these developments often translate into heightened anxieties about safety and personal security.[88] Many women remain cautious about sharing personal information online due to fears of harassment, identity theft, stalking, or misuse of their data. The lack of effective institutional safeguards further amplifies these concerns. In many contexts, women perceive digital platforms as environments where privacy protections are fragile and where abusive behaviour may occur with limited accountability. As a result, the digital sphere can simultaneously function as a site of empowerment and a space of vulnerability. Research increasingly indicates that women

[85] Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)
[86] Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)
[87] Brenner SW, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press 2012)
[88] Ibid.

encounter cybersecurity threats more frequently than men, particularly in the form of gender-based harassment.[89] One of the key factors contributing to this disparity is the absence of gender responsive policy frameworks within cybersecurity governance. Traditional cybersecurity approaches have primarily focused on protecting technological infrastructures such as networks, databases, and information systems. While such protection is essential, it often overlooks the human dimension of cyber threats, including the ways in which social inequalities shape digital risks.

The neglect of gender-specific concerns within cybersecurity policy is reflective of broader patterns in which issues related to privacy, safety, and bodily autonomy are marginalized within discussions of technological development. Debates about equality and justice frequently emphasize political representation or economic participation, yet the digital security of women remains insufficiently addressed.[90] In an era in which large segments of social interaction occur online, the absence of robust protections against digital harassment has significant implications for women's ability to participate freely in digital environments. Another factor that exacerbates women's vulnerability in digital spaces is the persistent digital literacy gap. Access to technological knowledge and cybersecurity awareness remains unevenly distributed across societies. In many regions, women face barriers to technological education and digital training, limiting their ability to recognize and respond to cyber threats.[91] Without adequate knowledge of privacy settings, secure communication practices, or data protection strategies, users may unknowingly expose themselves to exploitation. Addressing this gap requires targeted initiatives aimed at strengthening digital literacy, particularly among women and marginalized communities.

The gender disparities evident in contemporary digital spaces are also rooted in historical developments within the technology sector itself. Contrary to common perceptions, women played an important role in the early development of computing. During the early decades of computing history, programming was often regarded as routine clerical work and was performed largely by women. In fact, computing was sometimes described as a "pink-collar profession," reflecting the significant presence of women within the field. Female programmers and mathematicians made substantial contributions to technological innovation, particularly during the mid-twentieth century. Women's participation was especially visible during the Second World War, when female codebreakers and analysts played critical roles in decoding encrypted communications and supporting military intelligence operations. Their analytical skills and technical expertise were essential to wartime cryptographic efforts.[92] Despite these contributions, the professionalization of the technology sector gradually marginalized women's roles within computing. As computing became associated with higher levels of prestige, economic power, and technical specialization, gender stereotypes increasingly shaped hiring practices and workplace cultures. Women's expertise was often undervalued, and many were discouraged from pursuing long-term careers in

[89] Singer PW and Friedman A, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014)
[90] Brenner SW, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press 2012)
[91] Ibid.
[92] Deibert R, *Black Code: Surveillance, Privacy and the Dark Side of the Internet* (Signal Books 2013)

science and technology. Over time, this shift contributed to the gender imbalance that continues to characterize the technology sector today. The cybersecurity industry, in particular, remains heavily male-dominated. Global estimates suggest that women constitute only a small proportion of the cybersecurity workforce. Although this figure has gradually increased over time, the gender gap remains substantial.

The limited representation of women within cybersecurity has important consequences for the development of digital security frameworks. Diversity within technological fields is crucial for addressing complex challenges, as different perspectives and experiences contribute to more comprehensive solutions. When women are underrepresented in decision-making roles, the specific vulnerabilities they face may remain overlooked within policy and technological design. The absence of female role models and mentors also discourages younger generations of women from pursuing careers in cybersecurity, perpetuating a cycle of underrepresentation. At the same time, the expansion of digital platforms has intensified various forms of cyber violence directed at women.[93] Online harassment, misogynistic abuse, and targeted hate campaigns have become increasingly visible in social media environments. Surveys conducted in different regions suggest that a significant proportion of women have experienced some form of online harassment. Female journalists, activists, academics, and public figures often face coordinated digital attacks designed to silence their voices and discourage participation in public debate.

Cyberstalking represents another significant dimension of gendered cyber insecurity. This form of abuse involves persistent monitoring or harassment through digital technologies, including unauthorized access to personal accounts, spyware installations, and location tracking through GPS-enabled devices. In many cases, cyberstalking occurs within intimate relationships, where abusive partners use technology as a tool of control. Digital surveillance can restrict victims' autonomy, undermine their sense of safety, and escalate into real-world threats. Non-consensual dissemination of intimate images has also emerged as a pervasive form of cyber violence. The unauthorized sharing of private photographs or videos—often referred to as revenge pornography—can have devastating consequences for victims. Women subjected to such violations frequently experience emotional trauma, social stigma, and reputational damage. In certain contexts, victims may face exclusion from professional or social networks, and in extreme cases they may even encounter rejection from their own families. Despite the severity of these harms, legal frameworks in many jurisdictions remain inadequate for addressing such offences effectively. Another increasingly prevalent practice is doxxing, which involves the public release of personal information such as home addresses, contact details, or workplace information without consent. By exposing victims' private data, perpetrators create conditions that facilitate harassment, intimidation, and physical threats. Women who advocate for gender rights or challenge patriarchal norms are particularly vulnerable to such attacks, which are often intended to silence dissent and discourage activism.

---

[93] Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

These patterns of abuse reveal how patriarchal norms and gender biases are reproduced within digital environments. Online misogyny often reflects broader cultural attitudes that seek to police women's behaviour and restrict their participation in public spaces. The normalization of such behaviour within digital cultures can discourage victims from reporting abuse, particularly when institutional responses are slow or ineffective. The consequences of cyber violence extend beyond immediate emotional harm. Persistent harassment can affect women's professional opportunities, economic independence, and willingness to engage in digital platforms that are increasingly essential for career development. Female entrepreneurs, journalists, and professionals often rely on digital tools for networking, communication, and business promotion. However, exposure to cyber harassment, identity theft, or privacy violations may discourage them from maintaining an active online presence. Women in developing regions face additional vulnerabilities due to limited access to technological resources and cybersecurity awareness. Structural inequalities in education, income, and digital infrastructure often restrict women's ability to benefit from technological advancements while simultaneously increasing their exposure to cyber risks. In such contexts, the digital divide intersects with gender inequality, reinforcing patterns of marginalization.[94] These dynamics highlight the importance of examining cybersecurity not only as a technological challenge but also as a social phenomenon shaped by power relations, institutional structures, and cultural norms. Understanding the gendered dimensions of cyber insecurity requires a broader analytical framework that situates digital threats within the context of structural inequality and social transformation. Such an approach opens the way for deeper exploration of how online violence operates, how institutional responses have evolved, and how gender-sensitive cybersecurity frameworks can be developed to address these emerging challenges in the contemporary digital era.[95]

Cybersecurity Governance and the Evolving Landscape of Global Digital Threats

The rapid digitalization of contemporary societies has transformed data, digital infrastructures, and interconnected networks into central components of economic activity, governance, and everyday life. As organizations, governments, and individuals increasingly rely on complex technological systems to conduct operations, the importance of cybersecurity governance has grown substantially.[96] Cybersecurity governance broadly refers to the institutional frameworks, policies, and decision-making processes through which organizations manage cyber risks, protect digital assets, and ensure compliance with legal and regulatory standards. It functions as the strategic backbone of cybersecurity management by establishing accountability structures, clarifying responsibilities, and aligning security practices with broader organizational objectives. In an era characterized by accelerating digital transformation, cybersecurity governance has become indispensable for maintaining operational continuity, safeguarding sensitive information, and strengthening resilience against increasingly sophisticated cyber threats. At its core, cybersecurity governance provides a systematic approach to identifying, assessing, and mitigating cyber risks. It encompasses the development of policies, oversight mechanisms, and risk management strategies

[94] Floridi L, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford University Press 2014)
[95] Ibid.
[96] MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012)

that enable organizations to protect their digital infrastructure and respond effectively to emerging threats. Without effective governance structures, cybersecurity initiatives often remain fragmented, leaving critical gaps that can be exploited by malicious actors. By defining clear roles and responsibilities and integrating cybersecurity into broader organizational strategies, governance frameworks enable institutions to adopt proactive rather than reactive approaches to digital risk management. In doing so, they help organizations anticipate vulnerabilities, strengthen defence mechanisms, and ensure that cybersecurity remains aligned with institutional priorities and regulatory requirements.

The significance of cybersecurity governance has become more pronounced as the digital landscape continues to expand in scale and complexity. The increasing reliance on interconnected systems, cloud-based services, and digital platforms has created a highly integrated technological ecosystem in which vulnerabilities in one component can rapidly cascade across multiple networks. In such an environment, cyberattacks can have far-reaching consequences, affecting not only individual organizations but also entire industries and national infrastructures. Effective governance frameworks therefore play a crucial role in coordinating security strategies, ensuring regulatory compliance, and fostering collabouration among stakeholders responsible for protecting digital systems.[97] One of the primary functions of cybersecurity governance is to address the growing risks associated with cybercrime and data privacy violations. The absence of coherent governance structures often results in inconsistent security policies and inadequate risk management practices, creating opportunities for cybercriminals to exploit weaknesses in digital systems. By establishing standardized procedures for risk assessment, incident response, and compliance monitoring, governance frameworks help organizations minimize exposure to cyber threats while maintaining transparency and accountability. Furthermore, effective governance strengthens trust between organizations and their stakeholders by demonstrating a commitment to safeguarding sensitive information and protecting user privacy.[69] The expanding digital ecosystem has simultaneously intensified concerns regarding the protection of personal and organizational data. Data has become one of the most valuable assets in the modern economy, driving innovation, enabling personalized services, and facilitating strategic decision-making. However, the increasing volume and sensitivity of data collected by institutions also amplify the risks associated with unauthorized access, misuse, and breaches. Data protection has therefore emerged as a central concern within cybersecurity governance, requiring robust frameworks capable of balancing security, privacy, and technological innovation.[70]

The contemporary cybersecurity landscape is marked by a growing number of sophisticated and large-scale cyber incidents that reveal the vulnerabilities inherent in interconnected digital infrastructures. High-profile attacks in recent years have underscored the systemic risks associated with weak cybersecurity governance. Incidents such as the SolarWinds supply chain breach and the ransomware attack on the Colonial Pipeline illustrate how cyber threats can disrupt critical infrastructure, compromise sensitive information, and inflict substantial financial and reputational

---

[97] MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012)
[69] Deibert R, *Black Code: Surveillance, Privacy and the Dark Side of the Internet* (Signal Books 2013) [70] Ibid.

damage.[98] These attacks not only exposed weaknesses in organizational security practices but also highlighted the broader implications of cyber vulnerabilities for national economies and public trust in digital systems. The economic consequences of cybercrime are particularly striking. Global estimates indicate that cybercrime imposes trillions of dollars in annual losses on the global economy, with projections suggesting that these costs will continue to rise as digitalization expands. Financial losses associated with cyberattacks include direct theft, ransom payments, operational disruptions, and the costs of recovery and remediation. However, the implications of cyber incidents extend far beyond immediate financial damage.[99] Data breaches and service disruptions can undermine public confidence in digital technologies, discourage technological adoption, and hinder innovation within digital economies. Cyberattacks targeting essential services further illustrate the societal implications of inadequate cybersecurity governance. Attacks on healthcare systems, for instance, can disrupt medical services and jeopardize patient safety by disabling critical information systems. The ransomware attack on Ireland's Health Service Executive demonstrated how cyber incidents can interfere with healthcare delivery, forcing hospitals to cancel procedures and delay treatments. Such incidents highlight the vulnerability of critical infrastructure sectors that rely heavily on digital systems for operational efficiency and service provision.[100]

Beyond economic and societal impacts, cybersecurity governance has also become a matter of national security. State-sponsored cyber operations have increasingly targeted government institutions, defence systems, and electoral processes, raising concerns about the use of cyberspace as a domain of geopolitical competition. Cyberattacks directed at energy infrastructure, communication networks, and financial systems can destabilize entire regions by disrupting essential services and undermining public confidence in national institutions. The coordinated cyberattacks on Ukraine's power grid during the mid-2010s demonstrated how cyber warfare can directly affect critical infrastructure, leaving millions without electricity and highlighting the strategic potential of cyber operations in modern conflicts.[101] Within this evolving threat landscape, cybercrime itself has become increasingly sophisticated and diversified. Among the most prevalent forms of cyber threats are ransomware attacks, phishing campaigns, and supply chain compromises, each exploiting different vulnerabilities within digital ecosystems. Ransomware attacks have expanded dramatically in scale and complexity, targeting organizations across sectors ranging from healthcare and education to energy and finance. These attacks involve malicious software that encrypts a victim's data and demands payment for its release. The global impact of ransomware was dramatically illustrated by the WannaCry attack in 2017, which affected hundreds of thousands of computer systems across multiple countries and disrupted critical services worldwide. In recent years, ransomware tactics have evolved to include "double

---

[98] Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

[99] Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

[100] Ibid.

[101] Greenberg A, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday 2019)

extortion," where attackers not only encrypt data but also threaten to publicly release sensitive information if ransom demands are not met.

Phishing attacks remain another highly effective method used by cybercriminals to infiltrate organizational networks. These attacks exploit human vulnerabilities rather than technical weaknesses, manipulating individuals into revealing confidential information such as login credentials or financial details. The increasing sophistication of phishing techniques—including spear phishing and business email compromise schemes—has made detection and prevention more challenging for organizations. Because phishing often relies on deception rather than technical intrusion, addressing such threats requires a combination of technological safeguards and user awareness initiatives. Supply chain attacks have emerged as particularly concerning threats within interconnected digital ecosystems. By targeting third-party vendors or service providers, attackers can infiltrate otherwise secure organizations and gain access to sensitive networks. The SolarWinds breach represents a striking example of how vulnerabilities within supply chains can be exploited to compromise thousands of organizations simultaneously, including government agencies and major corporations.[102] Such incidents illustrate how the interconnected nature of modern digital infrastructures creates systemic risks that extend far beyond individual institutions. Advanced persistent threats and state-sponsored cyber operations represent another dimension of contemporary cyber risk. These threats are typically characterized by long-term, stealthy infiltration of targeted systems, often aimed at extracting valuable intelligence or compromising strategic assets. Operations such as the Stuxnet attack on Iranian nuclear facilities demonstrated the potential of cyber tools to achieve strategic objectives traditionally associated with conventional military operations. Similarly, various state-linked hacking groups have been accused of conducting prolonged campaigns targeting intellectual property, industrial secrets, and government communications across multiple countries. Alongside these threats, the challenges of protecting data privacy have become increasingly complex. Data breaches have become a recurring feature of the digital age, exposing sensitive personal information such as financial records, health data, and identification details. Large-scale breaches affecting social media platforms and technology companies have demonstrated how vulnerabilities in data protection practices can expose millions of users to identity theft, fraud, and other forms of exploitation. Beyond the immediate consequences for affected individuals, such incidents also erode public trust in digital platforms and raise questions about the ethical responsibilities of organizations that collect and store vast amounts of personal data. Concerns about surveillance further complicate the relationship between cybersecurity governance and data privacy. Governments often justify extensive surveillance programs as necessary for national security and law enforcement purposes. However, these initiatives frequently raise concerns about the balance between security and individual privacy rights. Revelations regarding mass surveillance activities have intensified debates about the limits of governmental authority and the potential misuse of digital monitoring technologies. Similarly, corporate data collection practices—particularly those used for targeted

[102] Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013) [76] Ibid.

advertising and behavioural profiling—have raised ethical questions about consent, transparency, and the commercialization of personal information.[103]

The issue of informed consent is particularly significant in the context of digital data governance. Many users unknowingly agree to extensive data collection practices through complex terms of service agreements that are rarely read or fully understood. High-profile controversies involving the misuse of personal data for political or commercial purposes have highlighted the consequences of weak consent mechanisms and inadequate oversight. These developments have prompted policymakers in several jurisdictions to introduce regulatory frameworks aimed at strengthening data protection and empowering individuals with greater control over their information. Among the most influential regulatory initiatives are the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These frameworks have sought to enhance privacy protections by establishing stricter requirements for data collection, processing, and storage. The GDPR, in particular, has established a global benchmark for data governance by emphasizing principles such as user consent, data minimization, and the right to erasure. Its extraterritorial application has compelled organizations around the world to adopt stronger data protection measures when handling information belonging to European citizens. Similarly, the CCPA has expanded consumer rights in the United States by granting individuals greater control over how their personal data is accessed and used by corporations.[104] Despite these advances, the global cybersecurity governance landscape remains fragmented and uneven. One of the most significant challenges arises from the cross-border nature of cybercrime. Cyberattacks frequently involve perpetrators, victims, and digital infrastructures located in different jurisdictions, complicating efforts to investigate and prosecute offenders. Jurisdictional boundaries, differences in legal definitions of cybercrime, and the absence of harmonized regulatory frameworks often allow cybercriminals to exploit gaps in international enforcement mechanisms. Attacks such as the global spread of the NotPetya malware demonstrated how cyber incidents can affect organizations across dozens of countries while remaining difficult to attribute or prosecute effectively.

International cooperation initiatives have attempted to address these challenges by promoting collabourative approaches to cybersecurity governance. Agreements such as the Budapest Convention on Cybercrime provide frameworks for information sharing and coordinated law enforcement efforts. However, the effectiveness of such initiatives is limited by uneven participation and differing national priorities. Several major countries have not ratified these agreements, citing concerns about sovereignty and fairness in the development of international legal frameworks. As a result, global efforts to combat cybercrime remain constrained by geopolitical tensions and disparities in technological capabilities among nations. Emerging technologies such as artificial intelligence and the Internet of Things further complicate the governance landscape.[105] AI systems rely on large volumes of data to function effectively, raising

---

[103] Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

[104] Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)

[105] Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

concerns about transparency, bias, and accountability in automated decision-making processes. Meanwhile, the proliferation of IoT devices from smart home appliances to industrial sensors has introduced new vulnerabilities into digital networks. Many IoT devices are produced with minimal security features, making them attractive targets for cybercriminals seeking to exploit weaknesses in distributed networks. Incidents such as the Mirai botnet attack demonstrated how insecure IoT devices can be harnessed to launch large-scale distributed denial-of-service attacks capable of disrupting major internet services. These developments reveal significant gaps in existing cybersecurity governance frameworks. Many current policies focus primarily on reactive measures such as breach notifications and penalties rather than proactive strategies aimed at building resilience and preventing attacks. Small and medium-sized enterprises, in particular, often lack the

resources required to implement comprehensive cybersecurity programs, creating vulnerabilities that can be exploited by attackers. At the same time, regulatory fragmentation across jurisdictions continues to complicate compliance efforts for organizations operating in global digital markets.[106]

The growing nuances of cyber threats, the rapid evolution of digital technologies, and the persistent fragmentation of governance frameworks collectively underscore the need for more adaptive and coordinated approaches to cybersecurity governance. Addressing these challenges requires not only stronger regulatory frameworks but also greater international cooperation, improved technological safeguards, and sustained investment in capacity-building initiatives. Within this evolving context, a deeper examination of governance mechanisms, policy frameworks, and institutional responses becomes essential for understanding how digital security can be strengthened in an increasingly interconnected world. Cybercrime against women has increasingly emerged as a significant concern within global governance frameworks, particularly within the institutional architecture of the United Nations. As digital technologies expand across societies, the risks associated with cybercrime, online harassment, and digital exploitation have grown in scale and complexity. Women, in particular, experience disproportionate exposure to cyber threats due to existing social inequalities, gender-based discrimination, and structural barriers that shape their access to digital spaces. International organizations have therefore begun to recognize the gendered dimensions of cybersecurity and the urgent need to develop institutional responses that address online violence, digital exclusion, and technological vulnerabilities affecting women.

International and National Responses to Cybercrime Against Women

Within the United Nations system, the International Telecommunication Union (ITU) has played a pivotal role in addressing evolving technological risks. Established in 1865, the ITU is one of the oldest international organizations and has historically been responsible for coordinating global telecommunication standards and policies. Over time, its mandate has expanded to encompass broader issues related to digital governance and cybersecurity. As communication technologies evolved from telegraph networks to the contemporary internet-based ecosystem, the ITU increasingly acknowledged that cybersecurity is a foundational component of a safe and connected global society. The proliferation of malware, cyber espionage, cyber terrorism, and organized

[106] Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

digital crime has intensified concerns about the security of digital infrastructures. These developments have not only affected governments and institutions but have also created new vulnerabilities for individuals navigating online environments. Women are often disproportionately affected by such threats, particularly in the form of cyber harassment, identity theft, online stalking, and the non-consensual dissemination of personal content. Complementing the technological focus of the ITU, the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), established in 2010, has played a central role in addressing the gendered implications of digital insecurity. UN Women operates as the primary United Nations body dedicated to advancing gender equality, promoting women's rights, and supporting global efforts to eliminate violence against women. The organization also engages with issues affecting marginalized communities, including violence against LGBTQ+ individuals and gender minorities, particularly within digital spaces. Through its governance structure—

comprising an executive board representing different geographic regions—UN Women operates within the broader framework of the United Nations Charter to promote inclusive policies and gender-responsive strategies. In recent years, the organization has expanded its focus to include the intersection between gender, peace, and cybersecurity. Recognizing the growing role of digital technologies in shaping social and political life, UN Women initiated the "Women, Peace and Cybersecurity" project in 2021, aimed at enhancing women's participation in cybersecurity governance and promoting safer digital environments. Such initiatives reflect a broader acknowledgment that cybersecurity must incorporate gender-sensitive perspectives in order to address the distinct challenges faced by women in digital spaces. In 2024, UN Women further strengthened these efforts by launching a free e-learning platform designed to equip women with knowledge and practical skills relevant to the digital age. By providing accessible training resources, the initiative seeks to bridge the digital literacy gap and empower women to navigate technological environments with greater confidence and security. Alongside international efforts, national governments have also begun developing legal frameworks to address cybercrime against women.

In India, the rise in cyber offenses targeting women has prompted the development of a multilayered legislative architecture aimed at regulating digital conduct and protecting victims. The Information Technology Act, 2000 constitutes the primary legal instrument governing cyber offenses in India. It criminalizes activities such as hacking, identity theft, unauthorized access to digital systems, and electronic stalking. The Act also provides for the establishment of specialized cybercrime investigation cells that are tasked with addressing digital offenses more effectively. In addition to the IT Act, provisions within the Indian Penal Code (IPC) have been amended to address emerging forms of cyber-enabled violence. Legal provisions now cover offenses such as voyeurism, cyberstalking, and the non-consensual dissemination of intimate images, commonly referred to as "revenge pornography."[107] The Protection of Women from Domestic Violence Act, 2005 further extends protection to cases where digital technologies are used within abusive relationships to harass, threaten, or monitor victims. These legal instruments collectively reflect an

[107] Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

effort to adapt existing criminal justice frameworks to the realities of the digital era. Despite the existence of this normative legal structure, challenges related to enforcement, institutional capacity, and public awareness continue to limit its effectiveness. Many victims remain unaware of the legal protections available to them, while law enforcement agencies often face resource constraints and technical limitations when investigating cyber offenses. The gap between legislative provisions and their implementation therefore remains a significant obstacle to ensuring meaningful digital protection for women. Statistical trends further highlight the growing scale of the problem. Reports indicate that cybercrimes against women in India have increased steadily in recent years. In 2022 alone, the National Commission for Women reportedly received over 31,000 complaints related to crimes against women, including online harassment and digital abuse. Among these offenses, the non-consensual circulation of intimate images—commonly described as revenge pornography—has become one of the most disturbing manifestations of cyber violence. Such crimes not only violate personal privacy but also expose victims to severe psychological distress, social stigma, and reputational harm.

Indian law contains several provisions intended to address these forms of digital abuse. Section 72 of the Information Technology Act, 2000 criminalizes the unauthorized disclosure of personal information obtained through digital means. Any individual who discloses or publishes such information without consent may face imprisonment of up to three years, a monetary fine that may extend to five lakh rupees, or both. The provision emphasizes the protection of individual privacy and recognizes the harm caused by the misuse of personal data. The constitutional dimension of privacy protection was further strengthened in 2017 when the Supreme Court of India delivered its landmark judgment in *Justice K.S. Puttaswamy v. Union of India*. In this historic ruling, a ninejudge constitutional bench affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution, which guarantees the right to life and personal liberty.[108] The judgment marked a transformative moment in Indian constitutional jurisprudence by recognizing privacy as an essential component of human dignity and autonomy in the digital age. However, despite these legal and constitutional advancements, the persistence of cybercrime across Indian states illustrates the continuing challenges of translating legal protections into effective safeguards. Rapid digitalization, uneven access to cybersecurity awareness, and persistent gender inequalities contribute to an environment in which women remain vulnerable to online abuse. Consequently, addressing cybercrime against women requires not only stronger enforcement mechanisms but also sustained institutional efforts to enhance digital literacy, strengthen investigative capacity, and promote gender-sensitive approaches within cybersecurity governance.[109]

Conclusion

Despite the existence of an extensive statutory and institutional framework addressing cybercrime against women, the practical effectiveness of these mechanisms remains subject to critical scrutiny.

---

[108] Zuboff S, *The Age of Surveillance Capitalism* (PublicAffairs 2019)

[109] Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

The present analysis suggests that a significant gap persists between the normative strength of legal provisions and their operational implementation. India possesses a layered legal architecture that includes the Information Technology Act, 2000, relevant provisions of the Indian Penal Code, and specialized statutes such as the Protection of Women from Domestic Violence Act, 2005 and the POCSO Act, 2012. In addition, constitutional jurisprudence has reinforced the importance of privacy and dignity through the recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India (2017)*. Together, these instruments create a comprehensive legal framework that formally recognizes the seriousness of cyber violence and the need to safeguard women in digital spaces. However, the persistence and growing visibility of cyber offences indicate that the existence of legal protections alone does not necessarily translate into effective prevention or redress.

A closer examination reveals that the disparity between "law on the books" and "law in action" remains a defining challenge within India's cybersecurity governance framework. While legislative provisions criminalize acts such as identity theft, cyberstalking, voyeurism, and the non-consensual dissemination of intimate images, enforcement mechanisms often struggle to keep pace with the rapidly evolving nature of digital threats. Law enforcement agencies frequently encounter technical limitations, shortages of trained personnel, and jurisdictional complications when investigating cyber offences. The transnational nature of digital crimes further complicates prosecution, as perpetrators may operate across multiple jurisdictions while exploiting anonymity and technological sophistication. Consequently, victims often face procedural delays, difficulties in evidence collection, and limited institutional support, which collectively weaken the deterrent value of existing legal provisions. Statistical trends further underscore the complexity of the problem. Reported cases of cybercrime against women have increased steadily in recent years, reflecting a pattern that is simultaneously encouraging and concerning. On one hand, the rise in reported complaints may indicate growing awareness among women about their legal rights and greater willingness to approach institutional mechanisms such as the National Commission for Women or specialized cybercrime cells. On the other hand, the upward trajectory of these cases also suggests that cyber offences themselves are expanding in scale as digital technologies become more deeply embedded within everyday life. The proliferation of social media platforms, online financial services, remote work systems, and digital communication tools has transformed the internet into an indispensable infrastructure for modern living. In such a context, complete disengagement from digital environments is neither practical nor desirable. Women must participate in these spaces for education, employment, social interaction, and civic engagement. Yet this very participation simultaneously increases their visibility and accessibility within digital networks, often exposing them to new forms of vulnerability and exploitation.

This structural dependence on digital systems therefore creates a paradoxical condition. While digital technologies offer unprecedented opportunities for empowerment, connectivity, and economic participation, they also expand the terrain on which gender-based violence can occur. Cyber harassment, stalking, doxxing, and non-consensual image dissemination illustrate how traditional forms of gendered violence have migrated into digital environments, often amplified by the speed, anonymity, and reach of online platforms. Addressing these challenges requires moving beyond a narrow focus on statutory adequacy toward a broader examination of institutional readiness and governance capacity. It is essential to assess whether law enforcement agencies possess the technological infrastructure, investigative expertise, and gender-sensitive protocols

necessary to respond effectively to cyber offences. Equally important is the question of accountability. Violations may originate not only from individual offenders but also from systemic failures within institutions, regulatory frameworks, or digital platforms themselves. In such cases, the assumption of the state as an unequivocal protective actor becomes more complex and warrants careful scrutiny. Against this background, the chapter highlights the need for a multidimensional approach to cybersecurity governance that integrates legal, technological, and social perspectives. Ensuring meaningful digital safety for women requires sustained investment in institutional capacity-building, specialized cybercrime training for law enforcement agencies, and stronger coordination between regulatory bodies, technology companies, and civil society organizations. At the same time, initiatives aimed at strengthening digital literacy and cybersecurity awareness among women remain crucial for enabling individuals to recognize and respond to online threats.

Ultimately, it suggests that cybersecurity frameworks often function reactively rather than preventively. Regulatory mechanisms frequently emerge in response to technological disruptions rather than anticipating them. As digital innovation continues to accelerate, the gap between technological capability and regulatory adaptation may widen further unless proactive governance strategies are adopted. Evaluating the effectiveness of cybersecurity frameworks therefore requires asking whether they operate as genuine deterrents capable of preventing cyber offences or whether they primarily function as post-facto response systems activated only after harm has already occurred. This question forms a critical foundation for the subsequent analysis undertaken in this study, which seeks to examine how legal institutions, governance mechanisms, and technological systems can be strengthened to ensure that women's digital safety becomes a substantive reality rather than a merely aspirational promise in an increasingly technologized society.

----------**********----------

Chapter 5

Cybersecurity Risks in the Digitisation of Cultural Heritage in India: A Legal and Governance Analysis

Priyanka Das, Assistant Professor of Law, Swami Vivekananda University

Abstract

India is using digitization to both safeguard and promote the country's heritage through its cultural institutions like museums, manuscripts, archives, and other historical records. Digital forms of preservation are often considered a more secure and permanent way to preserve cultural assets, and many continue to subscribe to a larger myth associated with cybersecurity and how technology is assumed to be safe; therefore, this chapter will discuss if the current legal and governance framework created in India is sufficient to protect digitized cultural heritage from cyber-related threats. Most current literature discusses cultural heritage protection and cybersecurity governance in conjunction, but little existing analysis focuses directly on how current cybersecurity law applies to digital heritage institutions. This gap is important to note, as digital repositories become subject to various cyber threats, including data breaches, ransomware attacks, unplanned access via hacking, and weaknesses with the organizations that rely upon digital assets. This chapter uses doctrinal and analytical methods to review relevant laws related to this area of study, including but not limited to the IT Act, 2000, the Digital Personal Data Protection Bill 2023, and any other relevant heritage legislation and policy documents, along with secondary sources of information. By studying the intersection between digitization initiatives and cybersecurity regulatory initiatives, this study highlights the disparity between the intended benefits of digital preservation and the obstacles associated with cyber governance.

Keywords: *Digital Preservation, Cybersecurity Law, Cultural Heritage Protection, Data Governance, Institutional Vulnerability.*

Introduction

Cultural heritage is the artistic, scientific, or historical heritage of a culture or society. The term "cultural heritage" has various of definitions at both national and international level. However, it lacks any uniform definition. As per the UNESCO, "cultural heritage" includes "artefacts, monuments, a group of buildings and sites, museums that have a diversity of values including symbolic, historic, artistic, aesthetic, ethnological or anthropological, scientific and social significance. It includes tangible heritage, movable, immovable and underwater, intangible cultural heritage (ICH) embedded into cultural, and natural heritage artefacts, sites or monuments. The definition excludes ICH related to other cultural domains such as festivals, celebration etc. It covers industrial heritage and cave paintings."[110] The preservation of the immense variety of heritage has long been viewed as a priority for India, where numerous cultures have existed

[110] UNESCO Institute for Statistics, *2009 UNESCO Framework for Cultural Statistics (FCS)* (UNESCO 2009).

throughout its history. Historically, preservation was limited to the physical preservation of monuments and artefacts via statutory methods. However, digitalisation has become an emerging model of preserving and promoting cultural heritage in recent years. There has been a greater commitment to digitalisation as a preservation method because digitisation allows cultural institutions to convert tangible materials into digital formats, which makes for greater access to cultural heritage, promotes research opportunities, and helps prevent the degradation of fragile resources.[111]

In addition, the creation of digital repositories and archives allows for a greater possibility of public engagement through the access to cultural heritage, as well as allowing for new ways to document and disseminate cultural heritage. The result of this belief is that many people now trust that digital preserving solutions for the conservation of heritage will be the most reliable and secure option to meeting the difficulties of heritage conservation in the future. This trust reflects the confidence most people have in technology systems as providing a safe and long-term method for completing the process of preserving cultural, historical, or scientific heritage.

However, the assumption that digitisation automatically guarantees security overlooks the vulnerabilities associated with digital infrastructures. Cultural institutions that rely on digital platforms are exposed to cyber risks such as data breaches, ransomware attacks, unauthorised access and systemic institutional weaknesses. When heritage resources are integrated into digital environments, they become subject to the same threats that affect other information systems. Any compromise of digital heritage may have consequences that extend beyond operational disruption and may affect cultural continuity and public trust.

The Indian government has enacted legislation to deal with cyber issues. The legislation currently in place includes the Information Technology Act, of 2000 and the Digital Personal Data Protection Act, of 2023. The two laws set up a general framework to regulate cybercrime, but there has been very little attention given to how they are to be applied specifically to institutions with digitized cultural heritage. Most of the available literature on the issue has treated the two areas of research i.e Cultural Heritage Protection and Cyber Security as separate and neither area has had much in the way of scholarly examination that touches on the intersection between the two.[112]

The purpose of this chapter is to determine if current cyber governance and the legal framework in place in India is adequate to protect digitized Cultural Heritage from the potential of being harmed by cyber related threats. In order to accomplish this, this chapter will incorporate a doctrinal and analytical methodology in order to conduct an examination of the applicable statutes, legislation governing Heritage Sites, policy documents, and applicable secondary academic sources. This chapter will examine the applied relationship between digitized Cultural Heritage, digitization initiatives and Cyber Security Regulation, and will highlight gaps between the declared intent of

---

[111] Press Information Bureau, 'Digitization of Cultural Heritage in India' (17 March 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2111884&reg=3&lang=2 accessed 2 March 2026.

[112] DLA Piper, 'Data Protection Laws of the World: India – Data Protection in India' https://www.dlapiperdataprotection.com/?t=law&c=IN accessed 2 March 2026.

the policies and practices that are implemented to preserve Cultural Heritage Digitally and the challenges that exist in Nurturing Cyber Governance.

Digitisation of Cultural Heritage in India: Policy Context and Institutional Framework

India is working hard to create a digital representation of its cultural past. This is part of an initiative to create better government services and improve the uses of the internet. There has been a shift by many sources of cultural goods towards using computers to help preserve the information about their items, recording that information, and making it available to the public. The aims of these different agencies go beyond just needing to keep records, they want to provide access to their records, allow people to see them, and involve people once they have been made available.

Several successful projects have been supported by the Indian government to help digitise material.[113] All major projects have aimed to create online collections of items that could be used by everyone to learn about India's history. The national cultural institutions responsible for these projects include the National Archives of India, the Indira Gandhi National Centre for the Arts and various state museums. They have developed ways to scan and catalogue items digitally, so they can be accessed through various means online. The Digital India programme also emphasises the importance of electronic government and creates better digital infrastructure, which indirectly influences the cultural sector.

There are many benefits to digitisation. Digitisation aids in preserving delicate artefacts due to the decrease in physical handling of these items. Additionally, digitisation allows researchers, academics and the general public to have access to materials, regardless of geographic distance. Another benefit is that digitisation helps with documentation, and inventory management processes and therefore improves the administration efficiencies of institutions. Digital storage also permits duplication and backup, which potentially decreases the risk of irretrievable loss from natural disasters or deterioration of the physical object.

However, the digitisation of cultural assets results in a transformation of the cultural asset itself. Once in digital format, cultural heritage items are mere data format and stored on servers, networks and cloud systems. Consequently, protecting them will consist of information security functions rather than conservation functions. The risks associated with this changeover generally receive little or no attention. Cultural heritage institutions are generally underprepared for many digital security risks due to a lack of adequate cybersecurity infrastructure, or appropriate technical skill or financial resources to adequately manage digital threats.[114]

Also, third-party services are frequently engaged to support digitisation projects such as storage of data, software management, or cloud hosting, generating multiple futures for potential failure due

---

[113] Ministry of Culture, 'Digital Cultural Governance and Monitoring of Cultural Initiatives' (Press Information Bureau, 2 February 2026) https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2222115 accessed 2 March 2026.
[114] Samar I Bakhshi, 'Digitization and Digital Preservation of Cultural Heritage in India with Special Reference to IGNCA, New Delhi' (2016) 6(2) Asian Journal of Information Science and Technology 1, 2 https://ajist.co/index.php/ajist/article/view/134 accessed 2 March 2026.

to additional layers of vulnerability. Cultural heritage institutions may have weak contracts with third-party service providers, as well as poor security practices, and insufficient oversight leading to unauthorised access or use of digital data repositories. In some instances, cultural heritage institutions may not consider their digital collections to be valuable information assets, thereby limiting their investment in security measures.

Another important dimension concerns the value of cultural data. Digitised manuscripts, artefacts and archival records may contain sensitive historical information, indigenous knowledge systems or rare documentation. Such data may be attractive targets for cyber criminals, whether for financial gain, political motives or ideological reasons. Ransomware attacks, in particular, pose a serious threat because they can lock institutions out of their own collections unless payment is made. The loss or manipulation of cultural data may result in reputational damage and undermine public trust.

Policies governing digitalisation tend to put emphasis on growth/as well as access, with little thought given to Security arrangements. Most of the time, Innovation, and access are seen as high priority in relation to Technology, however, Security is viewed as secondary. Thus, there seems to be an implied belief that Digital Technologies, by virtue of being more advanced than other technologies, automatically provide Security. With the increased dependence on Digital Technology Infrastructures, one of the most important questions regarding Digital Heritage management will be whether or not the current legal and regulatory framework in India is sufficient for the Cybersecurity risks cultural institutions experience. In order to have an answer to this question, the appropriate statutes dealing with Cybercrime and Data Privacy should be reviewed and their relevance to the Heritage sector evaluated. This will be done in the following chapter.[115]

Cybersecurity Law in India and Its Applicability to Digital Heritage Institutions

Cybersecurity in India is primarily governed by legal regulation through the Information Technology Act of 2000, which was originally intended to enable e-commerce through the use of electronic signatures and provide a legal framework for e-businesses.[116] As it has evolved into a comprehensive piece of legislation, it now regulates various types of cyber-related misconduct, including cyber terrorism, as well as providing a legal framework for electronic records and electronic documents. The IT Act was amended to include provisions for data protection, victimisation and intermediary liability in 2008.

The IT Act includes several provisions that apply to digital cultural heritage institutions, including Section 43 that is unauthorised access to computer systems, theft of data and damage to computer systems and Section 66 that states about acts against computer systems that are done dishonestly or fraudulently. Both of these provisions would apply if a person accessed a digital archive or museum database without authorisation or altered, copied or deleted information from a digital

[115] National Archives of India, 'Information Technology' https://nationalarchives.nic.in/Information-Technology accessed 2 March 2026.
[116] 'Understanding the Information Technology Act, 2000 in E-commerce' (Lloyd Law College, 24 June 2025) https://www.lloydlawcollege.edu.in/blog/it-act-2000-ecommerce-legal-framework.html accessed 2 March 2026.

collection of cultural heritage. Additionally, Section 66F or cyber terrorism could become applicable if an attack on a cultural heritage repository creates a threat to national security or public order.

The objective of protecting sensitive personal information and requiring reasonable security practices with respect to sensitive personal data are among the several areas in which these two statutes overlap. While earlier regulations around Section 43A of the Act provided a basis for understanding how to meet the standards of data protection, the Digital Personal Data Protection Act of 2023 has now significantly enhanced this regulation by establishing a clear, structured system of providing adequate safeguards for processing personal data, including specifying the responsibilities and rights of individual data fiduciaries and data principals, respectively.

Although many cultural heritage organizations do not routinely have access or use large volumes of personal data, some archives or historical records may still contain information that is identifiable to persons, groups or communities who are the subjects of that collection.[117] This will therefore create a legal obligation to comply with all applicable provisions of the Act as it specifically relates to data processing activities and records. Rather, the primary and only purpose of most cultural heritage organizations that hold archival materials is to preserve and disseminate historical records, not to collect and store data for commercial purposes. Thus, it is highly debatable whether the cybersecurity requirements established pursuant to the Digital Personal Data Protection Act, 2023 satisfy the cybersecurity needs of cultural heritage organizations.[118]

The corporate and regulatory statutory provisions in India are only one of many systems for governing digital Heritage organizations and their controls. The National Computer Emergency Response Team functions under the authority of the Information Technology Act, which includes guidelines for reporting and responding to incidents related to cyber security. Many of the organizations outlined above operate digital systems and may be subject to reporting obligations established in the guidelines from N-CERT; however, the current level of awareness and compliance in this sector is unclear. The significant limitation within this existing framework is its general applicability. The Information Technology Act and Digital Personal Data Protection Act were designed and implemented across all sectors of the economy. Neither specifically identifies Digitized Cultural Heritage organizations as critical information infrastructure nor does either provide cultural repository organizations with sector-specific guidelines for implementing standards that enable the preservation of these types of collections.

This absence ultimately creates a situation where Digitized Cultural Heritage organizations must interpret the broad statutory provisions and statutory obligations on their own, without having access to meaningful assistance from the statutes. Moreover, cybersecurity governance requires more than just adherence to legal obligations. These organizations typically operate with limited

---

[117] T.K. Gireesh Kumar, 'Digital meets culture: towards a national portal for aggregating Indian cultural heritage' (2026)
Journal of Cultural Heritage Management and Sustainable Development 1, 5 https://doi.org/10.1108/JCHMSD-022024-0031 accessed 2 March 2026.
[118] DLA Piper (n 4).

technical capacity and financial means; therefore, even when statutory obligations exist, it may not be possible for them to properly implement those obligations. The difference between the formal protections provided by law and the institutional capacity to adhere to the law demonstrates a structural flaw within the existing systems.[119]

In summary, an analysis of the extent to which heritage specific laws and policies complement or contradict the wider cyber security framework must occur following this assessment. This will require that the intersection of cyber regulation with heritage protection laws in India.

Heritage Protection Laws and the Regulatory Disconnect in the Digital Context

Historically, the legal protection of India's cultural heritage has been aimed at preserving tangible monuments, sites and artefacts. The main legislation regarding the protection of ancient monuments is the Ancient Monuments and Archaeological Sites and Remains Act 1958. This Act primarily regulates and preserves monuments classified as being of 'national importance'. Another piece of legislation regarding antiquities is the Antiquities and Art Treasures Act 1972, which governs the export and trade in antiquities and art objects, amongst other things. Both pieces of legislation emphasise physical protection and regulatory oversight in the safeguarding of material heritage.

These pieces of legislation, while still important for protecting material heritage, are applicable only to the material heritage that existed before the rise of the internet and online technology. None of these statutes take into account the effects of digitisation and do not seek to provide for protection against hacking, data manipulation or the digital destruction of records. Once material culture has been converted to a digital format, it is no longer clearly covered by traditional heritage statutes.

The regulatory gap becomes apparent when we consider the holdings of archival and manuscript collections. Archival institutions, such as the National Archives, and public libraries operate from administrative structures and frameworks of rules, but these rules are usually more about custodial or facility responsibility than about securing the information that resides there.[120] Although many policy efforts have encouraged these institutions to digitize their manuscript and archival collections, there are currently few cybersecurity standards specifically tailored to their digital holdings.

This disconnection points to a larger systemic problem within the administrative framework for managing digital heritage. Heritage law and cybersecurity law exist in parallel with respect to the protection of cultural property versus addressing digital systems. Digital heritage occupies a hybrid reality that spans both areas of law. Digital heritage is, by nature, both a cultural good and,

[119] Ministry of Electronics and Information Technology, 'Digital India Programme' https://www.digitalindia.gov.in/ accessed 2 March 2026.
[120] National Archives of India (n 7).

therefore, a data resource. The lack of explicit legal recognition of digital heritage creates an incomplete and fragmented protection of this unique type of property.

In addition to ownership and authenticity, there are many other issues related to cultural materials in a digital environment including their copying, altering and redistributing. Questions about intellectual property rights and the moral rights of the original creator of the work are common; as are ethical questions about the integrity of digital reproductions. Although copyright law provides some protection from infringement, copyright law does not provide protections related to the broader security risks associated with unauthorised access or systemic cyberattacks on repositories.

In India, since cultural institutions are not generally classified as critical information infrastructure under the Indian cybersecurity policy, therefore cultural materials do not get the level of protection provided by the sector focus for critical infrastructure sectors such as finance, energy and telecommunications. Because damage to these critical infrastructure sectors has more immediate economic and security implications, the greater priority is to ensuring that they are able to operate without interruption or threat. Cultural heritage continues to be a significant part of a country's identity and helps to establish historical continuity, but they are often not perceived as being strategic targets for cyber-attacks. The perception of risk in this area may contribute to insufficient investment in cyber resilience for the cultural sector.

This regulatory disconnect operates on several levels: the statutory level, the institutional coordination level, and the level of government priorities. While within the area of heritage legislation there is not a requirement to conduct a digital risk assessment, there is also not any way for the cyber-security legislation to provide any protective measures for the heritage sector. Consequently, a regulatory framework that is designed to deal with cyber threats in general but fails to take into account or provide for the cultural significance of the information being protected.

Cybersecurity Risks and Governance Challenges in Digital Heritage

Acting as a bridge between digital and physical collections, cultural heritage institutions are digitising their manuscripts, artefacts, and archival records so that they are stored as digital assets in networked systems.[121] Even though improving access to collections and preserving collections through digitisation are invaluable benefits, digitisation puts cultural institutions at a higher risk of cybersecurity. A major cybersecurity concern facing cultural institutions is unauthorised access to a database that could allow a hacker to copy or change the digitised collection. This could put the authenticity and the integrity of the digitised collection at risk. Unlike physical damage, digital evidence of manipulation might not be readily apparent.

This creates long-term risks associated with the distortion of the historical record. Apart from the risk of unauthorised access, ransomware attacks present another serious concern.[122] If an attacker

---

[121] T.K. Gireesh Kumar, 'Digital meets culture: towards a national portal for aggregating Indian cultural heritage' (2026) Journal of Cultural Heritage Management and Sustainable Development 1, 3.
[122] CERT-In, 'Notes on Ransomware Prevention and Response' (2023) https://www.cert-in.org.in accessed 2 March 2026.

can encrypt digital repositories, institutions may have no way of recovering access to the digitised collections. If an institution does not have secure backups in place, this circumstance may result in the permanent loss of the digitised collection and could also result in reputational damage to the institution. Data that is inappropriately accessed can also create potential liability exposure for institutions if the archives contain personal or sensitive information.

Lastly, cultural institutions often operate with limited financial and technological resources. Portfolio risk may limit the priority given to cybersecurity at many museums and archives. Cultural institutions are often reliant on third party service providers for solutions related to cloud storage and database management, creating further complications when it comes to establishing responsibility and liability in the event of a breach.

Conclusion and Recommendations

The digitisation of India's cultural heritage is vital in preserving it, making it more accessible and allowing distribution of knowledge democratically. Digital methods also expand the audiences that can engage with historical materials and limit the physical deterioration of fragile items.[123] However, moving from traditional methods of preserving items to digital preservation involves a set of new vulnerabilities, which cannot be solved simply by advancing technology. As demonstrated through the analysis provided in this chapter, India has some comprehensive cybersecurity legislation; for example, the information technology Act 2000 and the Digital Personal Data Protection Act 2023 provide some protections for all sectors of industry.

However, neither the IT Act nor the Digital Personal Data Protection Act were written with the unique needs of institutions with digitally preserved cultural heritage in mind. In contrast, laws to support the preservation of cultural heritage institutions primarily address the physical preservation of cultural artifacts and do not adequately address the risks associated with the digital preservation of these items. This gap in laws exposes cultural repositories to the potential threat of losing access to cultural heritage through cyber-related incidents.[99]

Several approaches can be explored to close this divide. Firstly, guidelines providing policy direction for the digital heritage sector should be created, incorporating cybersecurity standards within strategies for cultural preservation. Secondly, heritage institutions must follow a set of minimum-security standards, including routine evaluations of risk, secure backup systems for data, and clear channels to report incidents related to cybersecurity. Thirdly, building capacity will provide staff within heritage institutions with a stronger technical knowledge of cyber-related hazards, as well as raise their level of awareness in relation to these risks.

Finally, it is essential that there is improved coordination between cultural bodies and cybersecurity agencies to clarify regulations and enhance institutional preparedness. Digitisation alone cannot be relied upon as the sole solution to the challenges of preservation; it needs to be backed by sufficient systems of governance that acknowledge digital heritage as an asset that is both cultural

---

[123] Sudipta Shee, 'Digital preservation of cultural heritage in India: A digital age' (2025) 7(1) International Journal of Humanities and Education Research 260. [99] DLA Piper (n 4).

and informational; protecting it calls for more than regulatory compliance institutions must demonstrate their ongoing commitment and co-ordinate their efforts through policies that all government entities support.

----------**********----------

Chapter 6

Artificial Intelligence in Banking and Ombudsman Services: Addressing Cybersecurity Challenges While Ensuring Justice

Dr. Souvik Dhar, Assistant Professor, School of Law, Brainware University

Abstract

This paper explores the transformative role of Artificial Intelligence (AI) and technology in banking and Ombudsman services. The research questions focus on identifying risks and proposing mitigation strategies for fair AI adoption. A qualitative methodology was adopted, analyzing legal statutes, literature, and expert opinions. The thematic analysis categorized risks into legal, technological, ethical, and operational domains. The paper discussed AI's integration into banking, highlighting customer support, fraud detection, personalized services, back-end automation, compliance, and cybersecurity. AI-driven chatbots and virtual assistants provide round-the-clock customer support, enhancing service efficiency and customer satisfaction. Fraud detection systems can analyze transactions in real-time, preventing financial crimes effectively. Personalized banking through automated advisors and hyper-personalization improves customer engagement. Back-end automation accelerates operations, reduces errors, and lowers costs. AI also streamlines regulatory reporting and strengthens cybersecurity defenses. These innovations collectively make banking faster, safer, and more customer-centric. The paper also critically examines risks associated with deploying AI in Banking Ombudsman services. It identifies legal challenges such as threats to natural justice and lack of explainability in AI decisions. Technological issues include bias, unreliability, and cybersecurity vulnerabilities. Ethical and institutional risks involve dehumanization, accountability gaps, and erosion of public trust. Regulatory gaps exist due to the absence of specific AI guidelines, risking exclusion of marginalized groups. Results indicate that while AI enhances efficiency, it also risks violating constitutional principles and data privacy. Biases inherited from training data can lead to discriminatory outcomes. Errors and cyber threats compromise decision reliability and data security. The lack of clear liability frameworks complicates accountability. The discussion emphasizes the need for human oversight, ethical guidelines, and regulatory reforms. Strengthening cybersecurity and establishing sector-specific regulations are crucial. Responsible deployment requires balancing innovation with safeguards. Developing AI and ensuring inclusive access are vital. Implementing legal and ethical frameworks will foster trust and justice. AI can significantly improve banking and Ombudsman services if risks are managed effectively. This paper aims to support policymakers, regulators, and financial institutions in fostering trustworthy AI systems. Ultimately, responsible AI use can promote equitable, efficient, and secure banking and dispute resolution services.

Keywords: *Artificial Intelligence; Banking system; Grievance redressal; Ombudsman; policy framework; cybersecurity.*

Introduction

The fast-paced evolution of technology, particularly Artificial Intelligence (AI), has significantly impacted the growth of various sectors around the world, with the banking sector being cited as one of the sectors that have been significantly impacted. The convergence of AI and the banking sector has, in effect, transformed the conventional banking system, resulting in increased efficiency, customer service, and security.[124] In the context of the country, the banking sector is undergoing a transformation, with the evolution of technology being the major contributor. Moreover, the Reserve Bank of India (RBI), which is the apex bank of the country, has been at the forefront in the promotion of the digital banking system, particularly the adoption of AI, through various measures.[125] Some of the measures include the introduction of AI-based innovations, including the use of chatbots, virtual assistants, biometric systems, etc.[126] These innovations have significantly impacted the growth of the banking system, resulting in the provision of faster, more efficient, and customer-centric services. These innovations have significantly impacted the growth of the banking system, resulting in the provision of faster, more efficient, and customer-centric services. Moreover, the evolution of technology has also had an indirect positive impact on the growth of the banking system, resulting in the promotion of financial inclusion.

The present study aims to investigate the application of AI in the banking sector and Ombudsman services, highlighting the legal, ethical, technological, and operational issues arising therefrom. While AI has the advantage of offering a plethora of benefits, it also poses a number of risks, particularly in the context of cybersecurity, data privacy, bias, and transparency, among others. The application of AI in critical sectors, such as dispute resolution and customer grievances, necessitates a high level of oversight to avoid the infringement of constitutional rights, particularly the right to privacy, and the principles of natural justice.[127] The Banking Ombudsman Scheme, introduced by the RBI, is a vital instrument in the resolution of customer grievances against banks. Traditionally, the Banking Ombudsman Scheme has relied on manual and paper-based documentation. However, with the emergence of AI and digital technologies, there is a tremendous opportunity to transform the existing system, with a view to increasing the efficiency, transparency, and accessibility of the system, although the application of AI in quasi-judicial and administrative functions poses a number of issues, which are critical and require due consideration.

From the academic and legal viewpoints, there is an immediate need for exploring the interface of AI, banking law, and the constitutional framework, especially in the context of the Indian scenario.

---

[124] Shyam Sunder Agrawal, Ninu Rose and K. Prabhu Sahai, 'The fintech revolution: AI's role in disrupting traditional banking and financial services' (2024) 7(1) Decision Making: Applications in Management and Engineering 243.

[125] P Kumar and Rishi Manrai, 'A study on accelerating digital financial inclusion for positioning India through AIenabled banking services' (2024) 6(4) International Journal for Multidisciplinary Research.

[126] S Agarwal, B Agarwal, and R Gupta, "Chatbots and virtual assistants: a bibliometric analysis," Library Hi Tech, vol. 40, no. 4, 2022, pp. 1013-1030.

[127] D. Leslie, C. Burr, M. Aitken, J. Cowls, M. Katell, and M. Briggs, 'Artificial intelligence, human rights, democracy, and the rule of law: a primer', arXiv preprint arXiv:2104.04147, 2021. [104] Justice K.S. Puttaswamy v. Union of India, AIR 2018 SC (SUPP) 1841.

The landmark judgment in Justice K.S. Puttaswamy v. Union of India[104] recognized the right to privacy as an integral aspect of the fundamental right under Article 21 of the Indian Constitution. This underlines the need for the legal framework to ensure the handling of data and the use of AI in the context of dispute resolution in the banking sector.

In the current paper, the legal, ethical, and operational aspects of the integration of AI in the banking sector and the Ombudsman schemes in the Indian context are explored. The focus of the paper is to explore the scope of the use of AI in the context of dispute resolution in the banking sector, while ensuring the constitutional rights of the parties involved in the dispute resolution process.

Research Objectives

This paper aims to give an exhaustive overview of the use of AI in the banking system, including the Ombudsman service, in India. This study aims to critically analyze the myriad implications of the use of AI in the banking sector and the Ombudsman schemes in the Indian legal and regulatory scenario. The objectives of the study are as follows:

1. Analyse the existing legal and regulatory scenario in the context of the use of AI in Indian banking services: This would involve the critical examination of the laws, guidelines, and judicial pronouncements applicable to the use of AI in the context of data privacy and dispute resolution laws and the constitutional provisions in the Indian context.

2. Evaluate the Banking Ombudsman Scheme in the context of the use of AI in the digital age.

3. Identify and critically examine the legal and ethical issues that are linked to the integration of AI in the banking system of dispute resolution.

4. Propose the legal and policy changes that are required to ensure the responsible use of AI in the banking system, including the Ombudsman service.

5. Examine the need for the incorporation of cybersecurity in AI-based banking systems.

Materials and Methods

The methodology that is being followed in this study is doctrinal, qualitative, based on legal analysis, interpretive approaches, and comparative perspectives. The aim is to arrive at an in-depth understanding of the legal and ethical principles that govern the use of AI in the context of banking, along with the dispute resolution mechanisms, particularly in the context of India.

Primary Data Sources

1. Statutes and Regulations:

The basic legal instruments would include the Reserve Bank of India Act, 1934, Banking Regulation Act, 1949, Information Technology Act, 2000, and the Digital Personal Data Protection

Act, 2023. These acts would provide the legal guidelines for banking operations, data protection, and digital dispute resolution. RBI guidelines, circulars, and notifications, such as RBI's Master Directions on 'Digital Payment Security Controls' and 'Integrated Ombudsman Scheme 2021,' would be critically analyzed to understand the current scenario in the country.

2. Judicial Decisions:

Important cases like the Justice K.S. Puttaswamy v. Union of India[128] would be the guiding principles for understanding the constitutional aspects of the right to privacy. Important cases would include Indian Medical Association v. Union of India[129], Shreya Singhal v. Union of India,[107]etc. These cases would be analyzed to understand the jurisprudence of the matter and the changing dynamics of the use of AI in the country.

3. Official Reports and Policy Documents:

Reports from the RBI, NITI Aayog, OECD, and other international agencies would provide the necessary context for understanding the changing dynamics of the use of AI in the country. RBI reports on fintech, digital banking, and the use of AI would be highly instrumental in understanding the perspectives of the RBI.

4. Case Law and International Jurisprudence:

The study would include the regulations of other nations like the European Union's regulations under the GDPR and AI Act, Singapore's regulations on the use of AI, and the UK's regulatory sandbox initiatives.

Secondary Data Sources

1. Academic Literature:

We will use journal articles, commentaries, and research papers to shed lighter and challenge the underlying principles of law, the technology issues, and the ethical issues involved.

2. Legal Commentaries and Textbooks:

We will use commentaries and textbooks on banking law, data privacy, and AI ethics to support the underlying principles of law and legal discussions.

Research Techniques

1) Legal and Doctrinal Analysis:

---

[128] Justice K.S. Puttaswamy v. Union of India, AIR 2018 SC (SUPP) 1841
[129] Indian Medical Association vs Union Of India & Ors., AIR 2011 SUPREME COURT 2365
[107] Shreya Singhal vs U.O.I, AIR 2015 SUPREME COURT 1523.

The core of the work will involve the interpretation of the legal provisions to understand the implications of the legal principles in the context of AI in banking and grievance redressal. This will involve an in-depth study of the legal provisions with a critical eye.

2) Comparative Analysis:

The study will also cover the legal frameworks in other jurisdictions to identify the best practices that could be adopted in the Indian legal system.

3) Critical and Thematic Analysis:

The study will cover the risks of bias, opacity, and breaches in the context of AI in banking and grievance redressal, along with the other issues that are connected with the use of AI. This will cover the implications of the use of AI in the context of the legal principles of fairness, transparency, etc.

4) Policy and Regulatory Framework Development:

The study will cover the development of the policy in the context of the legal provisions with the help of the doctrinal study and the comparative study.

5) Interdisciplinary Approach:

The study will cover the different aspects of the use of AI in banking and grievance redressal with the help of the different disciplines.

Limitations

In the context of the nascent stage of legislation related to the field of AI in Indian law, the study relies upon existing laws, judicial decisions, and international best practices. The dynamic nature of the technology and the law in the field of AI implies that the study may require updating in the near future with the enactment of fresh laws. Further, empirical data in the field is limited, which underlines the theoretical nature of the study.

Literature Review

Today, AI has become a mainstay in the lives of various sectors, with banking leading the way. In the past few years, there has been a lot of research and expert opinion on the role of AI in the banking sector, how it is changing the way banking is done, and how it is speeding things up, making it safer, and providing a more personalized service, though there are also risks and challenges that come with the adoption of AI. In this paper, a literature review on the role of AI in the banking sector will be presented, highlighting the benefits, the challenges, the legal and ethical issues, and the role of AI in dispute resolution and customer service.

Benefits of AI in Banking

Many experts are in agreement that AI has a lot to offer to the banking sector. AI is able to help banks sort through large amounts of data in a fast and accurate manner.[130] Moreover, AI is able to help detect fraud in a timely manner, thereby increasing the safety of the customer.[131]

Chatbots and virtual assistants are some of the most popular AI applications used in the banking sector. For example, chatbots are able to communicate with customers online and assist them with a number of issues. For example, banks like HDFC, SBI, and ICICI have their own chatbots, which are referred to as Eva, SIA, and iPal, respectively.[132] These chatbots are able to operate around the clock, which means that the customer is able to get assistance at any time of the day or night. For example, a customer is able to get the status of a loan application or check the account balance in a matter of a second, whereas in the past, the customer would have had to wait in a queue.[133]

Advantage of using AI in the banking sector is that it is able to provide the customer with a personalized banking experience. AI is able to help the customer plan their investments with the help of a robo-advisor, which is a device that is able to assist the customer in the creation of a plan to help them achieve their goals.[112] The robo-advisor is able to analyze the customer's goals, income, and risk tolerance and provide them with the best investment strategy. AI is able to read the customer's needs and provide them with the most appropriate services. If the customer is a fan of traveling, AI is able to provide them with a credit card that rewards them with miles.

Another advantage of the use of AI in the banking sector is that it is able to help the bank automate a number of back-end operations. The AI is able to help the bank open a number of accounts, verify the details of the customer, and verify the compliance of the customer with the rules and regulations of the bank.[134] For example, in case the customer wants to open an account with the bank or wants to take a loan, the AI is able to verify the details of the customer in a matter of a second.

The AI also helps the bank in following the rules that are set by the regulators. For example, the AI is able to scan the transactions in the bank to verify whether there is any money laundering or fraud activities going on in the bank. The AI is also able to help the bank in the preparation of the

---

[130] Suparna Biswas, Brant Carson, Violet Chung, Shwaitang Singh, and Renny Thomas, AI-bank of the future: Can banks meet the AI challenge (McKinsey & Company 2020) 28.

[131] Rahul Khurana, 'Fraud detection in ecommerce payment systems: The role of predictive AI in real-time transaction security and risk management', International Journal of Applied Machine Learning and Computational Intelligence, vol. 10, no. 6, 2020, pp. 1-32.

[132] Kanika Sachdeva, and Meenakshi Dhingra, 'Role of Bank Chatbots in Managing Business during Crisis: A Study of Customers' Perceptions of ICICI Bank and SBI Bank', in Building Resilience in Global Business During Crisis, pp. 38-57. Routledge India, 2024.

[133] Everestus Obinwanne Eze, and Adaora Darlingtina Odunukwe, 'On application of queuing models to customers management in banking system', American Research Journal of Bio Sciences, vol. 1, no. 2, 2015, pp. 14-20. [112] P. Sironi, FinTech innovation: from robo-advisors to goal based investing and gamification. John Wiley & Sons, 2016.

[134] Abdel-Rahman Layla, and Yuli Andriansyah, 'The role of artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance', Reviews of Contemporary Business Analytics, vol. 6, no. 1, 2023, pp. 110-132.

reports that are to be submitted to the regulators.[135] This way, the AI is able to ensure that the bank is within the law, which is very important in the current digital world.

Risks of Using AI

Despite the many advantages associated with AI, a significant number of researchers and experts also raise concerns about the possible disadvantages of AI. One of the main disadvantages of AI is the bias associated with it. AI learns and makes decisions based on the data available to it, and if the data is biased, it is possible that AI will also be biased in its decision-making process.[136] For example, if AI is trained with historical data indicating that certain groups of customers are less likely to obtain loans, AI may end up denying loans to those customers disproportionately in the future, thereby encouraging discrimination and unfair treatment of certain classes of customers.

The lack of transparency is also a major disadvantage of AI. AI, particularly deep learning, is a black box, and it is difficult to understand how AI makes decisions.[137] In banking and other areas such as dispute resolution, it is essential for decisions to be transparent so that customers or clients understand the rationale for the decision and, as such, are able to put their trust in AI. AI decisions, if they are not transparent, may also be deemed unfair and against the principles of natural justice.

The other major disadvantage of AI is the lack of data privacy associated with it. AI needs a significant amount of data to make decisions, and this data may include customers' personal information, which may be compromised if AI is mishandled, thereby damaging customers and creating a lack of trust in AI. Experts are of the opinion that data protection legislation is necessary to protect customers' data.

Cybersecurity is another challenge. As AI tools become more advanced, hackers also try to find ways to attack banking systems. Cyberattacks like hacking, phishing, or ransomware can cause huge losses. AI can help prevent some attacks, but it can also be used by hackers to create smarter attacks. Therefore, cybersecurity measures must keep up with AI advancements.

Regulatory gaps are also a problem. Many countries, including India, lack clear rules about how AI should be used in banking. Without proper laws, there is a risk that AI could be misused or cause harm. Experts suggest creating specific laws and guidelines to regulate AI use, especially in areas like dispute resolution.

AI in Dispute Resolution and Customer Service

The role of AI is also being increasingly used in the resolution of customer complaints and disputes. A significant research literature suggests that AI may facilitate the resolution of customer complaints and disputes by speeding up the process of handling customer complaints and

---

[135] Jon Truby, Rafael Brown, and Andrew Dahdal, 'Banking on AI: Mandating a proactive approach to AI regulation in the financial sector', Law and Financial Markets Review, vol. 14, no. 2, 2020, pp. 110-120.

[136] Adheesh Kadiresan, Yuvraj Baweja, and Obi Ogbanufe, 'Bias in AI-based decision-making', in Bridging Human Intelligence and Artificial Intelligence, pp. 275-285. Cham: Springer International Publishing, 2022.

[137] Arun Rai, 'Explainable AI: From black box to glass box', Journal of the Academy of Marketing Science, vol. 48, no. 1, 2020, pp. 137-141.

disputes.[138] This can be done by categorization of complaints, prioritization of urgent complaints, and even providing possible solutions for customer complaints and disputes. Accordingly, the time taken to resolve customer complaints and disputes is reduced, and customer satisfaction is improved.

Some concerns remain with regards to issues of fairness and justice in the resolution of customer complaints and disputes, such as those in the Indian context, where the Banking Ombudsman Scheme is available for customers to raise complaints against banks. Earlier, the process of resolving customer complaints and disputes is manual, where human officials listen to customer complaints and disputes and make decisions. The incorporation of AI may facilitate the resolution of customer complaints and disputes by aiding in the categorization of customer complaints, providing initial responses, and even understanding patterns in customer complaints and disputes.

However, some researchers suggest that AI should not be exclusively used for the resolution of customer complaints and disputes,[139] as it does not understand human emotions and context, as observed in the resolution of disputes, where human relationships and context play a major role in the resolution of customer complaints and disputes. Secondly, fairness and absence of bias in AI decisions also remain a concern, and AI should be used as a supporting tool for human decisionmakers rather than exclusively using AI for the resolution of customer complaints and disputes.[119]

Legal and Ethical Issues

Many researchers stress the importance of the protection of constitutional rights, especially the right to privacy under Article 21 of the Indian Constitution. The judgment in the landmark case of Justice K.S. Puttaswamy v. Union of India[140] recognized the right to privacy as a fundamental right. This places the responsibility upon the banks and the regulatory agencies to ensure that the use of AI applications complies with the right to privacy by ensuring the use of personal information with the consent of the parties involved. Therefore, the use of AI must comply with the principles of the right to privacy.

Another issue that needs to be considered is the issue of transparency and interpretability. The ability of clients to understand the decisions made by the AI system needs to be considered. This is because the use of an uninterpretable decision made by the AI system would be in contravention of the principles of natural justice, which emphasize the right to be heard in the decision-making process. Ethical issues in the use of AI are many, especially the issue of discrimination. Many researchers stress the importance of auditing the use of AI in order to ensure that the use of the

---

[138] Sonali Chadha, and Sid Sirisukha, 'Empowering Indian banks–AI powered dispute resolution for better customer service', ICL Journal, 2024, p. 85.
[139] Muhammad Ali Malik, 'The Effect of AI Powered Sentiment Analysis on Consumer Complaint Resolution in Ecommerce: A Comparative Study of Human Vs AI Meditation Support', PhD diss., Business Studies, 2024. [119] Moses Alabi. "Ethical implications of AI: bias, fairness, and transparency." Computer Science and Engineering (2024).
[140] Justice K.S. Puttaswamy v. Union of India, AIR 2018 SC (SUPP) 1841.

technology is fair and non-discriminatory. This is because the use of AI technology in the financial sector could unjustly discriminate against certain classes of people in society, thereby exacerbating the social inequality that already exists in society.

Another issue that needs to be considered in the use of AI in the financial sector is the issue of accountability. This is because the error in the decision made by the AI system could be attributed to many parties, including the developer of the system, the financial institution, and the regulatory agency. Therefore, the development of the use of the technology needs to be well understood in order to ensure the use of the technology in the financial sector.

International Perspectives and Best Practices

There are many countries working on developing regulatory guidelines and standards for AI systems. The European Union, for example, has introduced the AI Act, which categorizes AI systems based on risk and sets rules for high-risk AI applications, including those used in justice and finance systems.[141] Singapore has developed its national AI governance framework, which prioritizes transparency, fairness, and safety.[142]

India can take inspiration from these international developments. There are experts who have recommended developing local laws and ethics for AI systems used in banking, with the intention of ensuring that technology is used for the greater good of all citizens and their rights are protected.

Results and Discussion

Drawing from extensive literature, legal frameworks, case laws, and expert opinions, the discussion here explores how AI transforms banking operations, enhances dispute resolution, and raises critical legal and ethical issues. The discussion seeks to emphasize the critical point that, even as the use of AI in the banking sector enhances efficiency, accessibility, and personalization, it presents critical risks that need to be regulated properly.

The study indicates that AI has redefined the operations of the banking sector in many ways, resulting in critical efficiencies in the operations of the sector. In particular, the study discloses that AI tools, such as chatbots and virtual assistants, are integral components of the contemporary banking sector.[143]

Enhanced Customer Support and Accessibility

One of the most prominent benefits of AI is its ability to provide round-the-clock customer service through chatbots and virtual assistants. Banks such as SBI, ICICI, and HDFC have developed their

---

[141] Anat Keller, Clara Martins Pereira, and Martinho Lucas Pires, 'The European Union's approach to artificial intelligence and the challenge of financial systemic risk', in Multidisciplinary perspectives on artificial intelligence and the law, pp. 415–439. Cham: Springer International Publishing, 2023.
[142] Philip L. Frana, 'Assessing Smart Nation Singapore as an international model for AI responsibility', International Journal on Responsibility, 7, no. 1 (2024): 2.
[143] Margherita Mori, 'AI-powered virtual assistants in the realms of banking and financial services', (2021).

own AI-powered chatbots—SIA, iPal, and Eva—that respond instantly to customer queries. These tools handle a large volume of routine questions, such as checking account balances, transaction history, or loan status, significantly reducing waiting times and improving customer satisfaction. The deployment of AI in customer support has made banking services more accessible, especially in a vast and diverse country like India.[144] Customers in remote areas or with limited digital literacy can receive assistance via multilingual AI interfaces, ensuring inclusivity. AI-based virtual assistants also help overcome language barriers, catering to India's linguistic diversity.

Personalization and Financial Advisory

AI enhances customer engagement through hyper-personalization. Robo-advisors analyze individual financial data, preferences, and risk profiles to recommend tailored investment options and savings plans. This democratizes wealth management, making sophisticated financial advice available to a broader audience at a lower cost.

Banks leverage AI to offer targeted marketing, customized credit offers, and personalized product suggestions.[145] This not only improves customer experience but also results in increased loyalty and retention. Such personalized services foster a more inclusive financial environment by catering to diverse customer needs.

Fraud Detection and Risk Management

AI systems excel at analyzing large datasets for detecting suspicious activities and potential fraud in real-time.[146] For instance, AI algorithms monitor transactions for anomalies, such as unusual login locations or sudden large withdrawals, and alert banks immediately. This proactive approach enhances security, reduces losses, and builds customer trust.

In credit risk assessment, AI models evaluate multiple data points—social media activity, transaction history, and behavioral patterns—to make faster and more accurate lending decisions. This facilitates financial inclusion by extending credit to individuals with limited credit histories, provided the AI models are designed fairly.

Automation of Back-End Processes and Compliance

AI automates routine back-end operations such as account opening, verification, and compliance checks, significantly reducing operational costs and human errors.[147] Robotic Process Automation (RPA) handles repetitive tasks efficiently, freeing human resources for more complex

---

[144] Khusboo Mittal, 'Leveraging Artificial Intelligence to enhance customer service in cooperative banks in India', (2025).

[145] Chandrima Bhattacharya, and Manish Sinha, 'The role of artificial intelligence in banking for leveraging customer experience', Australasian Accounting, Business and Finance Journal, 16, no. 5 (2022).

[146] N. Al, Faisal, Janifer Nahar, Niger Sultana, and Abdul Awal Mintoo, 'Fraud detection in banking leveraging AI to identify and prevent fraudulent activities in real-time', Journal of Machine Learning, Data Engineering and Data Science, 1, no. 01 (2024), pp. 181–197.

[147] Robert N. Boute, Joren Gijsbrechts, and Jan A. Van Mieghem, 'Digital lean operations: Smart automation and artificial intelligence in financial services', in Innovative Technology at the Interface of Finance and Operations: Volume I, pp. 175–188. Cham: Springer International Publishing, 2021.

decisionmaking.[148] Furthermore, AI supports regulatory compliance by automating the monitoring of transactions for anti-money laundering (AML) and combating the financing of terrorism (CFT).[149] AI-driven systems generate timely alerts, ensuring banks adhere to legal requirements and avoid penalties. AI enhances cybersecurity by continuously monitoring network activity, identifying threats, and responding to cyberattacks swiftly.[150] Biometric authentication, facial recognition, and fingerprint scans powered by AI improve security and reduce fraud, making digital banking safer.

Challenges of AI Integration

Despite the numerous benefits, the research identifies significant challenges and risks associated with AI in banking, especially concerning legal, ethical, and operational aspects.

Algorithmic Bias and Discrimination

One of the most critical concerns is bias inherited from training data. AI systems, if not properly designed, can perpetuate existing social biases, leading to unfair treatment of certain groups. For example, AI models used for credit scoring might unfairly deny loans to marginalized communities if historical data reflects discriminatory practices. Research highlights those biases in AI can violate principles of equality and non-discrimination enshrined in constitutional and legal frameworks. Regular audits, diverse data training, and transparent algorithms are necessary to mitigate this risk.

Lack of Transparency

Many advanced AI models, particularly deep learning algorithms, operate as "black boxes," making their decision-making processes opaque. Customers and regulators demand explainability, especially in sensitive areas like dispute resolution and credit approval.

The inability to explain AI decisions can violate the principles of natural justice, which require that decisions affecting individuals' rights be transparent and justifiable. Courts and regulators are increasingly scrutinizing the explainability of AI systems, emphasizing the need for human oversight and interpretable models.

---

[148] C. Vijai, and M. Mariyappan, 'Robotic Process Automation (RPA) in human resource functions', Advances In Management, no. 16 (2023), p. 3.
[149] Georgios Pavlidis, 'Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era', Journal of Money Laundering Control, vol. 26, no. 7 (2023), pp. 155–166.
[150] Goutham Sunkara, 'AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks', Well Testing Journal, vol. 31, no. 1 (2022), pp. 185–198.

Data Privacy and Security Concerns

AI systems require vast amounts of personal and financial data, raising concerns about privacy breaches and misuse. The recent case of data breaches and cyberattacks illustrates the vulnerability of banking systems to malicious actors.

India's evolving data protection laws, such as the Digital Personal Data Protection Act, 2023, aim to address these concerns. However, the lack of comprehensive legal safeguards and enforcement mechanisms remains a challenge, which could undermine customer trust and violate constitutional rights like privacy under Article 21.

Regulatory Gaps and Lack of Legal Frameworks

The research finds that India lacks specific regulations governing AI use in banking and dispute resolution. Existing laws are inadequate to address issues such as liability for AI errors, accountability, and standards for ethical AI deployment.

International models like the European Union's proposed AI Act and Singapore's AI governance framework provide useful references. India needs to develop sector-specific guidelines and oversight bodies to ensure responsible AI adoption.

Cybersecurity Threats

As AI becomes more integrated into banking systems, cybercriminals also exploit vulnerabilities. AI-driven cyberattacks, such as ransomware and phishing, threaten the security of customer data and financial assets.

While AI can strengthen cybersecurity, over-reliance on automated systems without robust safeguards can lead to vulnerabilities.[151] Continuous updates, threat intelligence, and human oversight are essential to counteract evolving cyber threats.

Digital Divide and Inclusivity

The deployment of AI-based systems might unintentionally exclude marginalized groups lacking digital literacy, internet access, or regional language support. This digital divide undermines the goal of financial inclusion and equitable access to grievance redressal mechanisms.[152] AI interfaces need to be designed with inclusivity in mind, incorporating regional languages, accessible formats, and offline options.

---

[151] Khang, Alex, ed., AI-Powered Cybersecurity for Banking and Finance: How to Enhance Security, Protect Data, and Prevent Attacks (CRC Press, 2025).

[152] Abhijit Ghosh and Ankita Bhatia, 'Bridging the Digital Divide: Leveraging Technological Innovations for Inclusive and Sustainable Finance', Financial Innovation for Global Sustainability (2025), pp. 305–336.
[133] Justice K.S. Puttaswamy v. Union of India, AIR 2018 SC (SUPP) 1841.

Judicial and Legal Developments

The judiciary in India has played a vital role in shaping the legal landscape related to AI, privacy, and digital evidence. Landmark cases like Justice K.S. Puttaswamy affirm the constitutional right to privacy, emphasizing that data collection and processing by AI systems must respect individual rights.[133]

Courts have increasingly recognized that AI decisions must be fair, transparent, and accountable. Judicial decisions have also clarified that electronic evidence, such as transaction logs and chatbot transcripts, must be supported by proper certification to be admissible in courts, which is crucial for AI-driven dispute resolution. The courts are also examining the scope of natural justice in AI-based decisions, emphasizing that decisions must be explainable and provide individuals with a fair opportunity to be heard. As AI becomes more prevalent, judicial scrutiny will intensify to ensure that technological innovations do not violate constitutional principles.

Recommendations

The research indicates that AI's future in Indian banking and dispute resolution is promising but requires careful regulation and oversight. Policymakers should develop comprehensive legal frameworks that address AI-specific issues such as liability, bias, explainability, and data privacy. Establishing regulatory sandboxes, as seen in the UK and Singapore, can facilitate experimentation with AI while ensuring compliance with safety standards. International best practices suggest that AI governance should be based on principles of transparency, fairness, accountability, and inclusivity. Regular audits, impact assessments, and stakeholder engagement are necessary to monitor AI systems' performance and address emerging risks. Building awareness among consumers about their rights and the role of AI in banking will foster trust and confidence. Finally, a hybrid model combining AI automation with human oversight is recommended. Human judgment is vital in complex disputes, ensuring that decisions are empathetic, fair, and legally sound.

Conclusion

Research and expert opinions agree that AI has great potential to transform banking and dispute resolution in India. Its benefits include faster services, better fraud detection, personalized advice, and improved regulatory compliance. However, risks related to bias, transparency, privacy, and accountability must be carefully managed. Creating clear laws, ethical standards, and oversight mechanisms is crucial for responsible AI use. Regular audits, transparency in decision-making, and human oversight are necessary to ensure fairness and justice. International best practices can serve as models for India to develop a balanced approach that harnesses AI's power while protecting citizens' rights. Overall, the literature emphasizes that AI can bring many benefits to banking and dispute resolution if used responsibly. The focus should be on creating an inclusive, fair, and safe environment where technology enhances trust and confidence in the financial system.

The integration of AI into banking and Ombudsman services offers immense potential to improve efficiency, accessibility, and customer satisfaction. However, the associated risks—bias, lack of transparency, data privacy, and legal gaps—must be addressed proactively. The legal and regulatory environment must evolve to keep pace with technological innovations, balancing progress with constitutional safeguards. As India advances in AI adoption, the focus should be on responsible innovation, ensuring that AI serves justice, promotes financial inclusion, and upholds individual rights. The future of AI in banking depends on creating a resilient, transparent, and inclusive ecosystem that leverages technology's benefits while safeguarding against its risks.

_____**********_____

Chapter 7

Digital Afterlives: Cyber Vulnerability and Social Belonging

Adrija Nath, Independent researcher, Jadavpur University

Abstract

In contemporary digital societies, cybersecurity is generally grounded as a technical problem, so much so that breaches are measured in financial losses, identity theft is reduced to credit score damage, and phishing is treated as a failure of awareness or digital literacy. Yet for those who experience hacking, impersonation, data breaches, or sudden deplatforming, the entire experience does not end when passwords are reset or accounts are restored. Instead, it initiates what this paper calls as a *digital afterlife* which is a chronic socio-psychological condition in which identity, their sense of belonging, and trust are reshaped by conditions of cyber vulnerability. This study moves the focus away from technical fixes to people's real-life experiences. It argues that cyber victimisation is not just about financial loss, but a deep disruption to a person's social life and sense of stability. Using in-depth interviews with people who have gone through hacking, identity theft, phishing scams, or being removed from online platforms, this study places these experiences within wider sociological ideas such as stigma, trauma, social identity, and trust in institutions. Drawing on Erving Goffman's idea of a "spoiled identity," the paper shows th1at many victims begin to blame themselves after such incidents. They often feel ashamed and describe themselves as careless, naïve, or lacking digital skills. These experiences show that it is not just personal embarrassment at play, but also a broader cultural belief that online safety is primarily an individual's responsibility. As a result, being a victim of cybercrime becomes a stigmatised condition, something people often keep hidden, rarely speak about openly, and one that is closely tied to judgments about a person's competence in the digital age.

The paper also tries to understands cyber victimisation as a kind of identity trauma. Unlike ordinary property crimes, digital breaches unsettle the line between who a person is and how they appear online. When someone's email is hacked, their social media is impersonated, or their account is suspended without any explanation. Their digital self, which in today's world is very central to work, relationships, and public life, becomes fragile and exposed. Participants describe feeling detached from themselves and exposed, almost like as if they have lost control over their own story and identity. Especially in cases of suspension of profiles, people describe a feeling of being erased from public life. Losing access to a platform is seen as a social exclusion from spaces where their friendships, work opportunities, and political voice are rooted.

The study also looks into how cyber vulnerability changes people's trust in institutions. Many victims describe a second layer of harm when they face unclear and unsupportive customer service systems, and a sense of bureaucratic indifference. Banks, online platforms, and government agencies often come across as distant, impersonal, and hard to deal with. As a result, people's trust in these institutions is often shaken. The effects of a breach therefore go beyond personal anxiety,

leading to a wider sense of doubt and mistrust toward the systems and institutions that govern digital life.

The study also reflects that the long-term effects of cyber incidents are not experienced equally. People with limited digital skills, insecure jobs and thus people who are marginalised socially often face stronger stigma and take much longer to recover. For instance, the freelance workers and content creators, when removed from a platform means endangering their livelihood. For women and people from marginalised gender identities, hacking and impersonation often bring extra reputational damage and moral scrutiny. Cyber vulnerability therefore works through the already existing social inequalities, making already precarious lives more unstable. Using ideas about social identity and trust in institutions, the paper argues that digital harm is deeply social and relational. By focusing on people's life experiences, the study questions mainstream cybersecurity approaches that mainly gives more importance to prevention and financial damage, while overlooking the difficult social recovery individuals go through after a digital violation. In terms of method, the study uses narrative analysis to follow how people tell the story of a cyber incident over time, from the initial shock and confusion to the longer-term ways they cope, with it. The digital aftermath is marked by a sense of tension, people still have to rely on digital systems in everyday life, yet they trust them much less than before. In the end, the paper argues that as more of our social, economic, and civic lives move onto digital platforms, cyber vulnerability should be understood as a serious form of social harm, not just a technical risk.

Keywords: *Cyber Vulnerability, Cyber Victimization, Extra Reputational Damage and Moral Scrutiny.*

Introduction

Digital technologies now shape much of everyday social life. Emails structure work routines in offices and institutions. Messaging platforms sustain friendships and maintain contact across distance. Social media profiles often function as public markers of identity where individuals present themselves to others. For many people, the internet is therefore not a separate space that exists outside social life. It has become one of the main arenas where relationships are maintained, reputations are built, and opportunities emerge. In this sense, digital presence is closely tied to how individuals are seen and recognised by others. Despite the growing importance of digital spaces in everyday life, discussions around cybersecurity are still framed largely as technical matters. When incidents such as hacking, phishing scams, identity theft, deplatforming are discussed, the focus usually falls on data protection, financial damage, or the need for better digital awareness. Institutional advice often centres on practical precautions such as creating stronger passwords or being more careful while using online platforms. While these measures are important, they also shape how cyber incidents are understood. They come to appear as problems that can be fixed once accounts are recovered or financial losses are managed, leaving little room to consider how such experiences might affect people beyond the immediate moment of the breach.

Yet these ways of thinking about cyber incidents leave out an important part of the story: how such events are actually experienced by the people who go through them. For someone whose account has been hacked or whose profile has suddenly been taken down, the experience rarely ends when

the technical issue is fixed. Many people continue to feel uneasy about their digital presence for some time afterwards. Some speak of embarrassment, especially when others become aware of what happened. Others describe a sense of exposure, as if something personal had been briefly taken out of their control. It is also common for people to begin questioning their own abilities with digital systems, wondering whether they missed some warning sign or made a mistake along the way. For a while after the incident, even routine actions online can feel slightly different. Activities that were once automatic may now be approached with caution.

This chapter approaches cyber incidents from this experiential perspective. Instead of looking at the technical side of hacking or data breaches, the focus here is on how individuals themselves understand and recount what happened to them. What matters is not only the incident, but what follows it. How do people make sense of such moments? How do they respond to the sudden awareness of vulnerability? And how does the experience slowly reshape the way they relate to the digital systems that are part of their everyday lives?

To describe this prolonged aftermath, the chapter introduces the idea of a *digital afterlife*. The phrase refers to the state in which people continue to live with the effects of a cyber breach even after the immediate disruption seems to have been resolved. When someone's account is hacked, their identity is impersonated, or they fall prey to cybercrimes, the event often leaves behind traces that linger for some time. People begin to see their digital identity differently. Their trust in the systems that organise online life may also change.

The chapter explores three central questions. First, how do individuals narrate their experiences of cyber victimisation? Second, in what ways do such incidents influence their sense of identity and belonging within digital spaces? Third, how do these experiences affect trust in institutions such as banks, online platforms, and other systems that organise digital life?

This chapter combines primary and secondary sources to explore how people experience cyber harm in everyday life. The primary data comes from qualitative interviews with individuals who had faced incidents such as hacked accounts, impersonation, cyber bullying or loss of access to digital platforms. These conversations focused on how participants understood and coped with these experiences in their daily lives. Alongside this, they also chapter draws on existing academic literature on digital identity, trust, and inequality. Bringing together personal accounts and scholarly work helped situate these experiences within the framework of social realities of life in a growing digital world.

The digital self and networked identity

Digital technologies have slowly become part of how people show themselves to others and stay connected in everyday life. Over time, these spaces begin to hold traces of everyday interactions such as messages, photographs, exchanges, payments, and memories. Because of this, digital accounts rarely feel separate from the individual who uses them. They become one of the ways through which people are recognised and remembered by others. Our digital presence today therefore, is much more than just a technical profile attached to a platform. It has become a part of how individuals see themselves and how they are seen by others.

Long before the rise of digital platforms, scholars such as *Erving Goffman*[153] suggested that everyday life involves a constant process of presenting oneself to others. People adjust how they speak, behave, and appear depending on the situation and the audience they face. A classroom, a workplace, or a gathering with friends each call for slightly different forms of self-presentation. Digital platforms extend this process into new settings. A profile page, a carefully chosen photograph, or a short biography now becomes part of how individuals introduce themselves to wider audiences. Even seemingly small choices like what to share and what to hide can shape how others perceive a person online. At the same time, these digital environments differ from earlier social settings as well. Interactions that once disappeared after the moment passed, now leave behind records that may remain visible for years. Messages, photographs, documents and posts accumulate over time, forming a kind of archive of a person's digital presence. This awareness often influences how people manage their online behaviour, encouraging a more careful form of self-presentation.

The growing importance of digital networks has also changed the spaces through which relationships are maintained. *Manuel Castell*[154]*s* describes contemporary societies as being increasingly organised through networks of information and communication technologies. Work relationships, friendships, public conversations, debates, shopping, transactions frequently unfold within these digital networks. Participation in such spaces is often necessary for staying relevant and connected with the world around us.

Anthony Giddens[155] too has offered a useful way of thinking about these developments through his idea of the "reflexive projection of the self." According to Giddens, individuals continuously reflect upon and shape their own life stories as they move through different experiences. Identity develops gradually through the choices people make, and the narratives they construct about themselves. Digital platforms have become one of the places now, where this process unfolds.

As a result, the boundary between online and offline life often becomes difficult to draw clearly.

Several participants in this study have described how closely their digital presence had become tied to their sense of everyday stability. One respondent, a freelance photographer in her late twenties, explained that most of her professional communication took place through a single email account and an online portfolio linked to social media. When she temporarily lost access to the account following a hacking attempt, she described the experience as deeply unsettling.

"It wasn't only about the account," she reflected during the interview. *"For a few days it felt like I had disappeared from the place where my work and contacts actually exist."*

---

[153] Erving Goffman, *The Presentation of Self in Everyday Life* (Penguin Books 1959).

[154] Manuel Castells, *The Rise of the Network Society* (2nd edn, Wiley-Blackwell 2010)

[155] Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age* (Polity Press 1991) [137] Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster 1995).

Sherry Turkle's[137] work on digital life offers a helpful way of thinking about how these spaces gradually become part of how people understand themselves. In her writings on life with computers and the internet, Turkle suggests that digital environments create new spaces where individuals can express and sometimes even experiment with different parts of their identity. Through conversations, posts, photographs, or messages, people begin to share fragments of their everyday lives online. Over time, these fragments form a visible presence through which others come to know them. Turkle points out that this process is not only about communication across distance. Online spaces also allow individuals to find communities that share similar interests, experiences, or concerns. Someone who feels unheard or unnoticed in one setting may find recognition in another digital space. And any disruption to this side of our lives gives meaning to what we can call a *digital afterlife* which is like a lingering condition that can follow a cyber incident long after the immediate problem appears to have been resolved.

Experiences of cyber victimisation are often accompanied by feelings that go beyond the immediate shock of the incident. Alongside confusion or anxiety, many individuals also describe a quieter emotion that surfaces soon afterwards that is embarrassment. Even when people recognise that they have been targeted by sophisticated scams or hacking attempts, they frequently speak as though the event reflects some personal mistake on their part. In conversations about cyber incidents, it is not uncommon to hear individuals describe themselves as having been "*careless*," "*naïve*," and "*not careful enough*." The language people use to recount these experiences often carries a tone of self-blame.

One way to understand this reaction is through Goffman's [156] discussion of stigma. He described stigma as a situation in which certain experiences or attributes come to be seen as discrediting within a particular social setting. When this happens, individuals may begin to feel that something about them has been judged negatively by others. They may try to conceal the experience or even internalise the judgement themselves. In such situations, the issue is not simply the event that took place, but the social meaning that is attached to it.

Cyber victimisation can easily take on this kind of meaning. In an environment where digital competence is increasingly taken for granted, people are often expected to know how to protect themselves online. Advice about cybersecurity regularly emphasises individual vigilance for instance recognising suspicious emails, avoiding unknown links, managing passwords carefully and report suspicious calls. While such guidance is important, it also creates a subtle expectation that responsible users should be able to avoid these risks. When something does go wrong, the incident can therefore feel less like a random misfortune and more like a personal lapse.

One participant in this study, a postgraduate student, recalled how uncomfortable she felt telling her friends that her email account had been compromised after she responded to a phishing message. Although she later realised that the email had been carefully designed to appear legitimate, her first reaction was embarrassment. During the interview she explained*:*

---

[156] Erving Goffman, *Stigma: Notes on the Management of Spoiled Identity* (Prentice-Hall 1963).

"I kept thinking I should have noticed something was wrong. It made me feel like I had been careless, even though the message looked very real at the time."

Another participant described a similar hesitation when discussing a social media account that had been temporarily taken over by someone impersonating him. Even after the account was recovered, he admitted that he had not told many people about the incident.

"It felt strange to talk about," he said. *"You start wondering what others will think. Maybe they will assume you weren't paying attention or you are a technological handicap"*

These reactions they show how cyber incidents can quickly become framed as individual failures. Instead of viewing themselves simply as victims of a crime, individuals may begin to interpret the event as evidence that they were not sufficiently cautious or knowledgeable. In Goffman's terms, the experience can threaten a person's sense of competence and produce what he described as a "*spoiled identity*." The individual may feel that something about their social image has been damaged, even if the incident itself was beyond their control. This sense of embarrassment often leads people to limit how openly they speak about what happened. Some respondents mentioned that they only told a small circle of close friends, while others avoided discussing the incident altogether. The reluctance to share these experiences is shaped partly by the fear of judgement.

One respondent, a young professional working in a technology-related field, spoke about how difficult it felt to admit that she had been the target of a phishing attempt that briefly compromised her account.

"*Because I work in a field where everyone is supposed to be digitally aware, it felt almost worse,"* she explained. *"I kept thinking that people would expect me to know better."*

Her reaction reveals how expectations surrounding digital competence can heighten this sense of personal failure when something goes wrong.

News reports and public campaigns frequently emphasise caution and awareness, sometimes implying that those who fall victim to scams may have ignored obvious warning signs. Although such messages aim to encourage safer online practices, they can unintentionally reinforce the belief that victims are responsible for their own misfortune. This cultural expectation is what places us in a difficult position making it an intersectional issue.

Identity Trauma and the Fragility of the Digital Self

When a cyber incident takes place, the first concern is often practical that is recovering the account securly and preventing further damage. Yet for many individuals, the experience does not end here. Over time, the incident can begin to affect how people think about their own digital presence and their sense of control over it. Digital accounts often hold much more than access to a platform and because of this, losing control over such an account can feel upsetting in ways that extend beyond technical control.

Anthony Giddens[157] understands this reaction through the idea of ontological security. He uses this term to describe the sense of stability that individuals rely upon to move through everyday life

with confidence. People develop routines and expectations that allow them to trust that the world around them will remain reasonably predictable. This sense of continuity is not always something individuals consciously think about; rather, it quietly supports the feeling that everyday life makes sense and remains under some degree of control. Digital systems have gradually become part of these everyday routines. Checking email, responding to messages, or logging into accounts or making online purchases or payments often happens almost automatically. Over time, these activities create a sense of familiarity with the digital environments people rely upon. Whenever there is a breach in this environment without warning, that sense of familiarity can be deranged. The experience can make individuals aware that something they once trusted can suddenly become uncertain.

Participants in this study when asked about this described this moment of disruption quite vividly. One respondent recalled discovering that someone had briefly gained access to her social media account and had begun sending messages to people in her contact list. Although the situation was resolved within a few hours, she described the experience as –

"For those few hours, I kept thinking that someone else was speaking as me. It felt strange to imagine that people might read those messages and think they came from me."

Such experiences point to the fragile boundary between a person and the digital representations through which others encounter them. When someone impersonates an account or gains access to a personal profile, that boundary becomes dimmed. The account continues to exist in public view, but the individual behind it may no longer have control over what appears there. In that moment, a digital identity can begin to feel detached from the person it represents.

Kai Erikson's[158] work on trauma provides another way to think about this sense of disruption. Erikson described trauma not simply as a response to physical harm but as an experience that shaken a person's sense of continuity and belonging. Trauma, creates a feeling that the familiar order of things has been disturbed. While cyber incidents differ greatly from the kinds of disasters Erikson originally wrote about, the underlying idea of disruption can still be useful. For some individuals, losing control over their digital identity produces a moment of disorientation. Accounts that once felt like stable extensions of their everyday life begin to appear fragile and uncertain.

Another participant described this experience after his professional email account was briefly compromised. Although no significant damage occurred, he remembered feeling uneasy even after the account was secured again. *"I kept thinking about how much of my work life is in that account,"* he said.

---

[157] Anthony Giddens, *The Consequences of Modernity* (Polity Press 1990).
[158] Kai Erikson, *Everything in Its Path: Destruction of Community in the Buffalo Creek Flood* (Simon & Schuster 1976).

"If someone can step into that space, even for a short time, it makes you realise how exposed things actually are."

Account suspension can produce a different but related feeling. In these cases, individuals do not lose control because someone else takes over their identity. Instead, they find themselves suddenly removed from a digital space where they previously had an active presence. One respondent explained that losing access to a platform where she had spent years sharing photographs and writings made her feel as though a small part of her social life had been abruptly cut off.

"It was strange," she reflected.

"It wasn't just about posting pictures. It felt like a place where my life had been unfolding had suddenly closed its doors."

These reactions they show how digital identities today, have become intertwined with everyday social interactions. Some participants also described a lingering awareness of vulnerability after the incident had passed. Even once accounts were recovered or secured, the earlier sense of certainty rarely returned in the same form. Routine activities such as logging in or sharing information began to carry a new layer of caution.

Institutional Trust and Bureaucratic Indifference

When people become victims of cyber incidents, the harm rarely ends with the initial breach. The experience often extends into a quieter struggle that involves navigating institutions that are supposed to help. Banks, online platform, customer support systems, and cybercrime authorities become the next points of contact. In theory, these organisations exist to restore order and protect individuals. In practice, many victims encounter something very different. Automated messages, complicated procedures, delays in follow ups and distant forms of communication t feel impersonal and slow. What begins as a technical problem quickly becomes a crisis of trust.

Trust plays a central role in how modern digital environments function. Individuals believe the systems managing their online activities are reliable. The idea of trust explored by *Niklas Luhmann*[159] helps explain this dynamic. Luhmann suggested that trust reduces complexity in everyday life. In a world filled with uncertainty, people rely on trusted institutions and systems so that they do not have to question every interaction or decision. Without this reliance, ordinary activities would become overwhelming. Digital infrastructures depend heavily on this kind of trust. Most users do not fully understand the technical mechanisms behind online platforms. Instead, they assume that these systems will work as promised. The presence of passwords, verification processes, and security alerts gives the impression that protection is built into the structure of the system. If things run smoothly, this trust remains largely invisible.

Problems arise when the system fails. A hacked account, fraudulent transaction, stolen identity or cyber bullying disrupts the quiet confidence people place in these systems. Suddenly, what once

[159] Niklas Luhmann, *Trust and Power* (John Wiley & Sons 1979)

felt routine becomes uncertain. At this moment, victims often turn to institutions for assistance. The expectation is simple that is someone will listen, investigate, and help restore what has been lost. However, the reality is quite different.

Let us consider the experience of contacting customer support after an online account has been compromised. Many platforms rely heavily on automated systems to manage large volumes of complaints. Victims are frequently directed through layers of help pages and chatbots before they reach an actual person, if they reach one at all. While these systems are designed for efficiency, they can feel deeply frustrating for someone who is already dealing with anxiety and confusion. The language of automated responses often sounds neutral and procedural, yet to victims it can appear dismissive or indifferent. A similar experience can emerge in interactions with banks following digital financial fraud. Victims may spend hours explaining their situation, submitting documentation, and waiting for internal investigations. During this period, uncertainty lingers. The individual is left wondering whether their money will be recovered, whether the institution believes their account of events, and whether the system truly prioritises their protection. Even when banks eventually resolve the issue, the process itself can leave a lingering sense of vulnerability.

The concept of trust in modern systems developed by *Anthony Giddens*[160] provides a useful way to understand this experience. Giddens argued that modern societies rely on what he called *"abstract systems"* which is a large, complex networks of expertise and technology that people depend on without fully understanding how they operate. For examples, we can take financial institutions, technological infrastructures, digital platforms and online payments. People interact with these systems daily, trusting that they are managed by competent experts. Cyber incidents expose the fragile nature of this reliance.

When something goes wrong, individuals suddenly confront the distance between themselves and the systems they depend on. The result is a feeling of disconnection. Victims may feel that their personal crisis has been absorbed into an impersonal administrative process. Further, interactions with cybercrime authorities can reinforce this sense of distance. Victims often describe feeling as though their experiences have been reduced to case numbers within a system that moves slowly and communicates little.

This bureaucratic character of institutional response can be better understood through the work of Max Weber[161]. Weber described bureaucracy as a rational organisational structure designed to maximise efficiency through rules, procedures, and hierarchies. Such systems are meant to produce consistency and fairness by treating cases according to standardised guidelines rather than personal judgement.

Yet bureaucracy has a paradoxical side. While its structured procedures are meant to ensure fairness, they can also produce emotional distance. Individuals facing urgent or distressing situations may feel that the system responds too slowly or too rigidly. The rules that keep

[160] Anthony Giddens, *The Consequences of Modernity* (Polity Press 1990) 27–29
[161] Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (University of California Press 1978).

institutions organised can also make them appear indifferent to the personal realities behind each case. This phenomenon can be described as secondary victimisation. The initial attack may involve financial loss, identity misuse, or the invasion of personal information. The institutional response, however, can unintentionally deepen the sense of vulnerability. Victims who struggle to obtain clear answers or timely support may begin to question whether the systems they trusted are truly capable of protecting them.

Inequality and Differential Cyber Vulnerability

Cyber harm is almost never socially neutral. While digital spaces often present themselves as open and universal, the risks and consequences attached to cyber incidents are quite unevenly distributed. People's social positions, play a significant role in determining how deeply they are affected. For some individuals, a cyber incident may be frustrating but manageable. For others, it can threaten their livelihood, reputation, or sense of safety. To understanding this uneven landscape it's important to grasp the of *digital divide*. This concept is not only about who has access to the internet but also about who feels confident accessing the digital systems. Individuals with strong digital literacy often recognise warning signs such as suspicious login alerts or phishing attempts. They may also know how to recover accounts, report incidents, or secure their information quickly. But those users who are less familiar with digital technologies often struggle to interpret what has happened or how to respond.

One participant, a 52-year-old tailoring service provider who had recently begun accepting online orders, described how difficult it was to deal with a phishing scam that compromised her messaging account:

"My customers started telling me they received messages asking for advance payments. I didn't even know someone had taken control of my account. My son had to sit with me and figure out what was happening."

Her experience reflects the uncertainty that can accompany limited digital familiarity. The breach itself was stressful, but the process of understanding the problem felt equally overwhelming. Instead of acting independently, she relied on younger family members to learn the technical aspects of account recovery.

Economic vulnerability also shapes how cyber incidents unfold. Freelancers and gig workers often depend entirely on digital platforms for visibility, payments, and client relationships. When these platforms malfunction or accounts become inaccessible, the consequences are immediate. One participant who worked as a freelance translator described how a security flag temporarily froze her payment account:

"The platform said they were reviewing my account for suspicious activity. During that time, I couldn't withdraw anything. I had already completed projects, but the money was stuck there. For two weeks I was just waiting and hoping they would clear it."

For her, the delay was not merely inconvenient. As someone without a fixed salary, access to that payment was crucial for covering monthly expenses. The platform's automated security measures, though designed to prevent fraud, ended up magnifying the precariousness of her situation.

Gendered expectations too influence how cyber harm is experienced. Several women participants spoke about the reputational anxieties that followed digital incidents. The fear was not simply about technical loss but about how others might see them. A postgraduate student described the distress she felt after discovering that someone had circulated edited screenshots of her social media posts in a private online group:

"They changed the captions and made it look like I had written things I never said. Even after I explained it was fake, I kept worrying about who had seen it."

In her case, the harm came less from the technological act itself and more from the social consequences attached to being the secondary sex. For individuals with marginalised gender identities, cyber incidents often intersect with the already present experiences of discrimination. Digital platforms may offer opportunities for visibility and connection, yet they can also become spaces where harassment and targeted attacks occur.

One interviewee, who identifies as a transgender man and runs a small online art page, described receiving repeated attempts by strangers to access his account:

"At first I thought it was random hacking attempts. But then I realised people were also sending messages saying things like 'people like you shouldn't be online.' That's when it started feeling personal."

The experience blurred the boundary between a technical threat and social hostility. What might have been let go as routine hacking attempts in another context became a question linked to his identity.

Another participant, a young non-binary student, spoke about the vulnerability of relying on online communities for emotional support:

"Most of my support system is online. When someone reported my account and it got temporarily restricted, I felt cut off from everyone who understood me."

For them, the platform was not just a communication tool but a crucial space for belonging. Losing access, even briefly, created a sense of isolation. These real life experiences reveal how cyber vulnerability is closely tied to broader social inequalities.

Living in the Digital Afterlife

Cyber incidents are often spoken about as - something goes wrong, the account is recovered, and life continues. But as we have understood for people the experience does not end when the technical part of it is resolved. The breach leaves behind a residual thought that their digital identity can be accessed, breached, altered, impersonated, and taken away without warning. The repercussion becomes a kind of *digital afterlife*. The event itself may pass, but the feeling remains.

For many victims, the experience begins with *shock*. The first moment of discovering that something is wrong rarely feels clear or immediate. Strange notifications, unfamiliar posts or unexpected transactions create confusion. Digital accounts usually feel stable and predictable, so the idea that someone else may be inside them is difficult to process. Once the reality of the breach becomes clearer, the emotional response often shifts inward. The second stage is quite often marked by *self-blame*. Instead of focusing only on the attacker or the system failure, individuals begin questioning their own behaviour. They wonder whether they could have done things differently. Even when cyber incidents are complex and difficult to prevent, victims often feel that they should have been more careful. This quiet sense of embarrassment can make people hesitant to talk openly about what happened.

After this comes a more practical but often frustrating phase which is the *struggle to regain control.* Individuals must deal with these platforms in order to recover their accounts or secure their information. While these processes are designed to protect users, they can feel slow and impersonal. The breach itself may have taken minutes, but the effort to repair its consequences can last much longer. Even after access is restored, many people find that their relationship with digital spaces has changed. A period of *social withdrawal* often follows. This does not always mean abandoning online platforms altogether, but participation becomes more cautious. People post less or think twice before engaging online. Activities that once felt effortless begin to carry a small sense of risk.

Over time, most individuals reach a stage of *adaptation.* They develop new habits which could be having stronger passwords, additional security settings, or more careful digital routines. These adjustments help restore a degree of stability, but they don't quite bring back the original sense of trust. Instead, digital life continues with a constant awareness that things can go wrong. In such a way, cyber harm often becomes less like a temporary interruption and more like a *chronic condition.*

Conclusion

Cyber incidents are often treated as technical mishaps. Yet the experiences discussed in this chapter suggest that the damage does not stay within the realm of tech. When a digital account is compromised, what is shaken is not just a platform but the person attached to it. Digital profiles today hold fragments of our identity. When these spaces are breached, the boundary between the self and its online representation suddenly feels brittle, leaving individuals feeling exposed or oddly detached from versions of themselves circulating online. At the same time, cyber incidents quietly reshape belonging. Because friendships, work, communities, and services now exist largely on platforms, losing access even briefly can feel like being locked out of a room where social life continues without you. The result is sometimes withdrawal, with individuals becoming more cautious about what they share and how they participate online from then on. These experiences also affect trust in institutions. Cyber vulnerability also tends to mirror existing inequalities- freelancers dependent on platforms risk losing income, individuals facing social scrutiny risk reputational damage, the differential experiences that comes with belonging from different social locations and digitally less literate users struggle more to regain control. For some, a breach is just an inconvenience but for many, it can deeply interrupt our everyday life.

These patterns reveal that cyber vulnerability is no longer just a technical risk but a social condition. As more of identity, work and relationships move onto digital platforms, cyber harm increasingly reflects broader structures of power, inequality, and institutional trust. In a world where so much of life unfolds online, protecting digital security is no longer just about better passwords or stronger firewalls rather it is about recognising cyber vulnerability as a form of *structural social harm* embedded within the very systems that organise contemporary social life.

_____**********_____

Chapter 8

Offence–Defence Asymmetry in the Age of Artificial Intelligence: Implications for the Cyber Threat Landscape

Apala Ghosh, PhD Research Scholar, Department of International Relations, Jadavpur University

Abstract

The swift integration of artificial intelligence (AI) into digital architecture is generally considered a transformative process in the area of cybersecurity. However, much of the current literature on the topic considers AI either as a technology that amplifies cyber capabilities or as a new form of governance challenge that demands regulation. This chapter presents a different case: that AI is best conceptualized as a structural variable that alters the balance of offence and defence in cyberspace. By using the theoretical framework of International Relations (IR) theory, specifically the literature on offence-defence asymmetry and security dilemmas, this chapter contends that the current form of AI systems aggravates the pre-existing imbalance between offence and defence in cyberspace, thereby exacerbating the instability of the global cyber threat environment. The offence-defence balance approach, which has traditionally been used to assess conventional and nuclear security, examines the prevailing technological and strategic conditions of a given environment to determine whether it is more advantageous to launch an attack or defend against one. When the costs of offence are lower than those of defence, states are likely to pursue preemptive strategies, the threat of escalation rises, and deterrence policy becomes unreliable. Cyberspace has long been considered an offence-preferred environment, where attackers need only find one vulnerability to breach the system, while defenders must protect a complex and constantly evolving target, where attribution is slow and uncertain, and where offensive capabilities can be easily copied at a low cost. The pre-AI cyber environment is already characterized by asymmetrical vulnerability. Cyber operations are different from traditional warfare in that they leverage systemic interconnectivity, civilian infrastructure, and dual-use technology. The defensive effort is high due to the expansive and constantly updated nature of digital networks, while the offensive community, whether state or non-state, enjoys the benefits of obscurity and anonymity. These characteristics establish what can be termed a persistent offence bias in cyberspace. The chapter will establish this baseline in order to evaluate the impact of AI on the balance and in which direction. Second, the chapter will explore how particular AI capabilities increase the reach of the offensive community. AI-enabled vulnerability scanning, code generation, and machine learning-driven reconnaissance decrease the technical skill set and time previously required for sophisticated cyber operations. Generative tools facilitate scalable and context-specific social engineering attacks, reducing the traditional trade-off between credibility and scalability in phishing and fraud. Adaptive malware can iterate independently in response to defensive efforts, improving the resilience and longevity of intrusions. Taken together, these trends reduce the barriers to entry for malicious actors, accelerate attack cycles, and improve the strategic reach of relatively resourceconstrained actors. Notably, the chapter will show how AI interacts with existing cyber structures to increase the flexibility of the offense. Third, the chapter will critically evaluate whether defensive AI mitigates

these trends. Advocates claim that machine learning improves anomaly detection, threat intelligence analysis, and real-time response capabilities. While these tools improve defensive monitoring, they are subject to structural and institutional constraints. Defensive AI systems require high-quality training data, produce a high rate of false positives, and require human direction within legal and administrative frameworks. Furthermore, defensive infrastructures are typically situated in complex public-private ecosystems, which impede coordination and response. By contrast, the offensive community enjoys fewer normative or institutional constraints. The imbalance is not only based on technical capability but also on organisational and regulatory environments that shape the use of AI. On the basis of this comparative analysis, the chapter goes on to examine the wider implications of international security. If AI further expands the offence defence gap in cyberspace, several implications follow. First, the risk of escalation could rise as the condensed time frames for detection and response leave less time for decision-makers to deliberate. Second, deterrence becomes more problematic as the delay between attacks and attribution trails the rapid execution of AI-enabled attacks. Third, the proliferation of superior capabilities to non-state actors further cloud state-centric visions of cyber stability. The chapter thus places AI in the context of debates on strategic stability, contending that cybersecurity must be understood not only as a technical challenge but also as a space of evolving power relations, and explores structural avenues for mitigating AI-driven asymmetry through architectural reform, collective defence coordination, improved attribution, and normative adaptation.The aim is to offer a framework by which policymakers and scholars might assess future technological developments without recourse to either alarmism or technological optimism.

Keywords: *Offense–Defence Asymmetry, Artificial Intelligence (AI), Cybersecurity, Cyber Conflict, Strategic Stability, Emerging Cyber Threats*

Introduction

The integration of artificial intelligence (AI) into digital infrastructure has been broadly described as a transformative moment for the field of cybersecurity. However, the current state of debate on this issue tends to vacillate between a vision of technological utopianism and a more alarmist vision of the future, without properly locating the phenomenon of AI within the existing body of literature on international security analysis. This chapter will contend that AI should not be considered simply a new "emergent risk" or "governance challenge" for cybersecurity. Rather, it should be considered a new "structural variable" that alters the balance of offence and defence in cyberspace.

The balance of offence and defence is a foundational concept in the field of International Relations (IR) theory, and it seeks to assess the prevailing strategic and technological conditions in a given international system as to whether they are more conducive to offensive or defensive action. When a system is characterised by a structural advantage for offence, this tends to increase the likelihood of escalation and undermine the stability of deterrence. Cyberspace has long been a system that is characterised by offence-preferential traits such as asymmetrical vulnerability, the difficulty of attribution, and the systemic interconnectedness of digital networks.

This chapter will argue that AI tends to further exacerbate these asymmetries by reducing the costs of innovation, increasing the tempo of operations, and diffusing advanced capabilities beyond the traditional state actor.

The main argument that will be made in this chapter is threefold. First, cyberspace is already a system that is characterised by a structural advantage for offence. Second, the current state of AI technology tends to increase this imbalance in a manner that is more pronounced on the side of offence than on the side of defence. Third, this has a number of implications for strategic stability, escalation, and the diffusion of power in international politics.

By locating the analysis of AI within the existing body of literature on offence-defence theory and applying it to the phenomenon of AI-enabled cyber operations, this chapter hopes to provide a more structured explanation of how technological change tends to alter the strategic equilibrium of international politics.

Section I

Reconsidering the Offence–Defence Balance in Cyberspace

The incorporation of artificial intelligence into digital systems has sparked an increasing amount of commentary speculating about the potential for transformation in the nature of cyber warfare. However, much of this literature is conducted without specifying the theoretical framework in which the potential for transformation is being measured. In order for AI to be considered a material factor, it must be considered not only as an innovation in technology but also as a factor within pre-existing frameworks of international security studies. Of these, the offence-defence balance is a particularly useful point of departure[162]. Rather than asking whether AI is "dangerous" or "useful," the offence-defence balance asks a more systematic question: does AI change the relative ease of attack and defence in cyberspace?

The offence-defence balance has long been used in the conventional and nuclear contexts. At its heart is a simple but profound observation: the balance between offence and defence determines the strategic incentives for conflict, arms racing, and strategic miscalculation. When offence is perceived to be superior, states are more likely to pursue pre-emptive strategies and to view defensive preparations as threatening. When defence is superior, the price of aggression increases and deterrence stabilizes strategic interaction. The balance itself is not simply a descriptive tool for military capability but shapes strategic behaviour through perception and expectation.

Applying this framework to cyberspace demands a nuanced conceptual translation. In contrast to territorial space, cyberspace is not geographically bounded but rather defined by its networked architecture. Occupation does not involve control of territory but rather access to systems and data. The relevant strategic question is therefore whether it is more structurally feasible to gain access to and exploit these networks than to comprehensively protect them. By this measure, the offence in cyberspace is simply gaining unauthorized access, obtaining or manipulating information, or disrupting its functionality. Defence is simply preventing unauthorized access, detecting intrusion, and restoring system integrity.

---

[162] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford University Press 2017).

Even before the advent of more sophisticated AI systems, cyberspace has shown characteristics that make defensive primacy difficult. Digital systems are complex and interconnected. Software development is a layered process, involving third-party libraries and constant updates. Each layer is potentially vulnerable. Because digital systems are constantly evolving, the defender must deal with an ever-expanding attack surface. The defender's problem is therefore systemic and ongoing. The attacker, on the other hand, needs only one point of vulnerability. This is not a guarantee of success, but it certainly establishes an asymmetry.

The balance of offence and defence in cyberspace is also affected by information asymmetry. Attribution of cyber-attacks is often difficult and delayed. Unlike conventional attacks, which often betray their origin through force projection, cyber-attacks can be routed through multiple sources and masked by technology. This makes deterrence credibility difficult to establish. If retaliation is dependent on successful attribution, and attribution is difficult or delayed, the cost of the offence is perceived to be lower. Structural ambiguity therefore combines with vulnerability to tip the balance in favour of the offence.

Nevertheless, the existence of an offence bias in cyberspace does not necessarily mean that innovation in defence is a futile endeavour. The balance between offence and defence is not static. Encryption protocols, multi-factor authentication, intrusion detection systems, and international norms have all changed the character of cyber engagement over time. The challenge is not to assert that cyberspace is necessarily offensive in nature, but to assess how technological change shapes relative costs.

Artificial intelligence must be placed in the context of this constantly shifting balance of power. AI systems improve pattern recognition, facilitate analysis, and support adaptive responses. These characteristics are dual-use. They can improve anomaly detection and defensive monitoring; they can also support automated reconnaissance, exploit development, and deception[163]. The strategic effects of AI depend on whether it upends the ratio of offensive to defensive effort. The role of effort must not be dismissed. In offence-defence theory, the key variable is not capability but cost. A technology that lowers the cost of performing offensive actions more than it lowers the cost of maintaining defence will shift the balance even if both sides are better off in absolute terms. Marginal change, not absolute change, is the key to structural advantage. In cyberspace, cost is more than just money. It includes time, expertise, coordination, and institutional constraint. Traditional cyber offence has required technical expertise and careful reconnaissance. Cyber defence requires constant monitoring, organizational coordination, and compliance with legal and regulatory requirements. In assessing the effects of AI, the key question is whether it changes these cost factors symmetrically.

A further conceptual clarification is needed on the role of technology and perception. The offencedefence balance of power theory highlights that what matters is not just material advantage but perceived advantage. If states perceive that AI-enabled cyber offence is gaining the upper hand, they may choose to counter by building their own cyber offence. These actions can create competitive spirals even in the absence of conclusive evidence that cyber offence has the

[163] Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment' (2017) 41 *International Security* 72.

advantage. In this way, AI can shape strategic stability through expectation effects as much as through capability effects.

Cyberspace also brings about complexities that do not exist in the traditional realm. Offensive and defensive capabilities can be the same. Research used for vulnerability identification for defensive patching can be used for offensive exploitation. Intelligence gathering for network defence is similar to intelligence gathering for attack. The dual-use nature of cyber capability makes it difficult to distinguish between the two, which were traditionally viewed as more distinct by offence-defence theory. AI makes this even more difficult because the machine learning models used for defensive anomaly detection can have the same underlying architecture as those used for offensive pattern recognition[164].

Moreover, cyberspace is inhabited not only by nation-states but also by corporations, criminal groups, and loosely connected collectives. The offence-defence balance thus applies at various levels of analysis. A technology that benefits non-state offensive actors can upset interstate relations indirectly. The spread of capability makes it difficult to apply traditional deterrence models, which rely on the existence of specific state-based adversaries. It is important to note that these complexities do not make the theory of offence and defence redundant. Rather, they highlight its versatility. The theory is a useful tool for examining the relationship between new technologies, incentives, and vulnerabilities. Rather than dwelling on the sensational implications of autonomous cyberwar, the offence-defence approach focuses on relative effort, scalability, and institutional constraints. The analytical argument made in this chapter is that artificial intelligence constitutes existing cyber asymmetries in ways that systematically favour offence. This argument is not based on technological determinism. Artificial intelligence does not necessarily enable attackers relative to defenders. Instead, it amplifies existing structural characteristics that already disadvantage defenders. Artificial intelligence decreases the marginal cost of reconnaissance, facilitates scalable deception, and accelerates adaptive exploitation, thereby reducing the marginal cost of offensive activities. Defensive systems are aided by artificial intelligence-assisted detection and response, but they remain limited by complexity and organizational factors.

The applicability of this argument extends beyond the technical realm of cybersecurity. If AI further exacerbates the offence-defence imbalance in cyberspace, it carries implications for strategic thinking among states[165]. Perceived vulnerability may lead to pre-emptive strategies, expanded offensive capabilities, and heightened suspicion. Conversely, if defensive innovation does not keep pace, confidence in digital security may erode, with attendant economic and political consequences.

---

[164] Henry Farrell and Abraham L Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 *International Security* 42.

[165] Martin C Libicki, *Cyber Deterrence and Cyberwar* (RAND Corporation 2009).

Section II

The Structural Foundations of Cyber Offence Advantage

Any hypothesis about the role of artificial intelligence in changing the balance of offence and defence in cyberspace must begin with a description of the underlying distribution of advantage. Otherwise, AI may be seen as the source of instability in itself, rather than a catalyst for the underlying conditions. The strategic nature of cyberspace was established well before the advent of massive machine learning systems. The architecture of cyberspace, its economic model, and its governance regime have created a space in which the superiority of defence has always been impossible to achieve.

The first structural basis for offence superiority is the architecture of digital systems themselves. Today's networks are not point solutions or self-contained systems. They are complex ecosystems that include operating systems, applications, firmware, third-party libraries, cloud infrastructure, and human interfaces. Each layer of the ecosystem introduces code, and each piece of code introduces the possibility of error. The size of today's digital systems ensures that vulnerabilities are not exceptional but statistical certainties. In such an environment, the defender's job is not simply to defeat an attack but to sustain systemic integrity through a constantly shifting technological landscape.

This is an architectural truth that creates a deep asymmetry of effort. Defence must be comprehensive. Offence only needs to be selective. An attacker needs to find one vulnerability that has not been noticed; a defender has to protect thousands of possible points of entry. The asymmetry is not merely one of degree but of logic. Failure for defence can occur through a single mistake; failure for offence does not preclude another attack. Since the cost of multiple attacks is low, persistence becomes a feasible strategy for attack. The complexity of digital systems thus embeds asymmetry at the level of system design.

The second basis for offence superiority is found in the economics of software development and cybersecurity investment. Cyber systems are built in a competitive market environment that favours innovation, speed, and functionality. Security is often an afterthought. Patching vulnerabilities takes time and effort that does not produce direct revenue. For many actors in the private sector, cybersecurity is a cost centre rather than a strategic investment. This economic incentive structure creates an uneven defensive posture across sectors and borders.

Attacks are driven by a different economic model. The development of exploits can be directly monetized through ransomware, data exfiltration, or denial-of-service attacks. Black markets enable the trading of vulnerabilities and malware[166]. Once developed, exploit code can be repurposed and adapted at a low additional cost. The commoditization of offensive capabilities reduces barriers to entry and allows capability to be widely distributed outside of elite technical circles. In this way, the economics of the cyber domain favour successful exploitation over successful prevention.

---

[166] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

Third, the attribution challenge undermines the credibility of deterrence. In traditional military conflict, tracing the source of attack is often an immediate or physically traceable process based on evidence of force projection. Cyber-attacks can be masked through proxy servers, compromised hosts, and routing techniques. Attribution is often a probabilistic process rather than a certainty. Even when technical analysis points to a likely source, political factors can complicate public attribution and retaliation.

Deterrence requires a credible threat of retaliation. When attribution is uncertain or delayed, there is a risk of miscalculation in response. This generates strategic ambiguity. Such ambiguity can be exploited by offensive actors who operate below the threshold likely to provoke escalation. Espionage, data manipulation, and limited disruption can be conducted in ways that test defensive resolve without triggering overt confrontation. Structural uncertainty therefore reduces the expected cost of certain forms of cyber aggression.

Temporal dynamics further reinforce asymmetry. Cyber intrusions are often gradual and may remain undetected for extended periods. During this time, attackers conduct reconnaissance, map networks, and prepare for disruption. Detection frequently occurs only after significant compromise has already taken place. The delay between intrusion and response provides attackers with informational advantage. Even when ultimately effective, defensive measures are reactive.

The defender's temporal burden is one of constant vigilance. Monitoring, updating, auditing, and responding require sustained organisational effort. Offensive actors can choose the timing of engagement strategically and are not required to maintain continuous visibility. This asymmetry of engagement places structural strain on defensive institutions.

A further imbalance arises from the diffusion of capability among both state and non-state actors. Unlike nuclear or advanced conventional weapons, cyber capabilities do not depend on large-scale industrial infrastructure. Skilled individuals, small groups, and criminal enterprises can develop impactful tools. The dissemination of knowledge through online platforms and open-source repositories accelerates this process. As capability spreads, the number of potential adversaries expands. Defensive actors must therefore guard against a diverse spectrum of threats, ranging from state-sponsored units to opportunistic criminal networks.

This diversity complicates strategic stability. Traditional deterrence models assume identifiable adversaries with centralised command structures. In cyberspace, potential actors include loosely organised networks whose motivations may not align with geopolitical rationality. Even if states achieve mutual deterrence, non-state actors may operate outside those constraints. The structural consequence is increased unpredictability.

Institutional and normative constraints further shape asymmetry. Defensive cybersecurity, particularly in democratic contexts, is embedded within legal frameworks governing surveillance, data retention, and automated response. Security measures must be balanced against privacy and civil liberties. Offensive actors, especially criminal organisations and authoritarian regimes, often face fewer normative constraints. This divergence affects the speed and intensity with which capabilities can be deployed. While defenders operate within compliance regimes, attackers iterate with comparatively fewer restrictions.

Interdependence compounds these structural factors. Digital infrastructure supports financial systems, healthcare networks, energy grids, and public administration. Civilian and military domains are interconnected. A vulnerability in one sector can cascade across others. The interconnectedness that enhances economic efficiency simultaneously amplifies systemic risk. Offensive actors benefit from this condition, as disruption in a single node can generate disproportionate consequences.

Taken together, these structural features—architectural complexity, economic incentive misalignment, attribution difficulty, temporal asymmetry, diffusion of capability, institutional constraint, and systemic interdependence—have produced a cyber domain in which defence faces intrinsic burdens. This does not imply the inevitability of offensive dominance; defensive innovation has strengthened resilience in numerous contexts. Nevertheless, the underlying asymmetry endures.

Establishing this baseline is essential for evaluating the impact of artificial intelligence. In a structurally neutral domain, the dual-use character of AI might generate symmetrical enhancement. In a domain already inclined toward offence, however, technologies that reduce operational cost or accelerate exploitation are likely to magnify imbalance. The analytical task that follows is therefore to determine whether AI interacts with these structural conditions in ways that amplify offensive leverage more than defensive resilience, and whether such amplification reshapes strategic incentives at the international level.

Section III

Artificial Intelligence as an Asymmetry Multiplier

Artificial intelligence does not operate in a neutral strategic environment. Instead, it is superimposed upon a cyber environment already marked by architectural vulnerability, economic misalignment, attribution uncertainty, and temporal imbalance. The relevant question, therefore, is not whether AI enhances capability on both sides—it clearly does—but how it interacts with these pre-existing asymmetries to alter their scale or character. The argument advanced here is that AI functions as an asymmetry multiplier[167]. It does not create structural imbalance; rather, it amplifies it by reducing the marginal effort required for offensive action more substantially than it reduces the systemic burden of defence.

The concept of marginal effort is central to this claim. In strategic analysis, absolute increases in capability are less significant than relative reductions in cost. If both offence and defence become more sophisticated, the balance remains stable unless the cost structures shift unevenly. Artificial intelligence lowers specific categories of effort—time, labour, expertise, and iterative testing—associated with offensive cyber operations. Although defensive actors also benefit from automation, the structural constraints identified earlier limit the degree to which those benefits can counterbalance offensive acceleration.

One of the most consequential developments introduced by AI is the automation of analytical labour. Historically, cyber reconnaissance required extensive system mapping, code examination,

[167] Thomas Rid, *Cyber War Will Not Take Place* (Hurst 2013).

and behavioural analysis. Machine learning models excel at identifying patterns across vast datasets. When applied offensively, they can analyse code repositories, network metadata, and publicly available information at scales beyond manual capacity. The effect is not merely increased speed but reduced marginal cost. Expanding analysis to additional targets does not require proportional increases in personnel. Computational scaling substitutes for human scaling.

This development directly interacts with the architectural complexity of digital systems. Given that vulnerabilities are statistically inevitable in large-scale infrastructures, lowering the cost of discovering them produces disproportionate strategic effects. The defender's obligation remains comprehensive: all potential weaknesses must be addressed. The attacker's obligation is selective: a single viable point of entry is sufficient. AI reduces the cost of selectivity. As search becomes faster and less resource-intensive, the likelihood of identifying exploitable weaknesses rises without equivalent growth in expenditure. The asymmetry embedded in system design thereby becomes more readily exploitable.

Generative AI produces a comparable shift in the domain of social engineering. Cyber intrusions frequently rely not only on technical exploits but also on manipulation of human behaviour. Previously, a trade-off existed between scale and specificity: highly tailored deception required labour-intensive preparation, while mass campaigns sacrificed credibility. Generative language models collapse this trade-off by enabling contextually tailored communication at negligible marginal cost [168]. Offensive actors can replicate institutional tone, incorporate contextual references, and adapt language to cultural settings without extensive human intervention.

The strategic consequence is enhanced scalability. When credible deception can be reproduced algorithmically, the volume of high-quality intrusion attempts increases. Defensive filtering systems confront dynamic variation rather than static templates. Machine-generated diversity challenges detection mechanisms reliant on known patterns. While defensive AI can analyse linguistic anomalies, it must minimise disruption to legitimate communication. Excessive sensitivity generates operational friction and economic cost. Offensive actors, by contrast, can tolerate failed attempts; unsuccessful experimentation carries limited penalty. This asymmetry in tolerance for error reinforces the broader asymmetry in cost reduction.

AI-driven iterative adaptation further widens the imbalance. Defensive cybersecurity often depends on identifying malicious signatures and deploying patches, processes historically marked by temporal lag. AI-enabled offensive systems can compress adaptation cycles by generating behavioural variants in response to detection. An offensive model can iteratively adjust until it identifies configurations that evade monitoring. Defensive responses, however, remain embedded within institutional processes of validation, coordination, and network-wide deployment. The obligation to maintain system stability constrains the speed of adaptation. Offence benefits from agility, whereas defence bears responsibility for continuity.

Lowered expertise thresholds also reshape the strategic landscape. AI-assisted coding and vulnerability analysis tools reduce technical barriers to conducting sophisticated cyber operations.

---

[168] Brandon Valeriano and Ryan C Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press 2015).

While skilled actors remain important, the pool of potential participants expands as marginal expertise requirements decline. Capability diffusion accelerates. More actors can attempt intrusion with less specialised training. Defensive institutions cannot equivalently reduce expertise thresholds without increasing systemic risk; effective security monitoring demands precision and oversight. The asymmetry between experimentation and reliability becomes more pronounced as AI tools proliferate.

Institutional context magnifies these dynamics. Offensive actors—particularly criminal organisations and loosely regulated entities—can deploy AI tools rapidly and without extensive oversight. They are not constrained by privacy regulations, procurement procedures, or public accountability. Defensive institutions, especially in democratic states and corporate settings, must integrate AI within regulatory and ethical frameworks. Concerns regarding transparency, bias, and legality mediate implementation. These governance requirements slow deployment and limit operational aggressiveness. Even where defensive AI offers technical advantages, its use is filtered through institutional friction.

It would be analytically unsound to claim that AI renders defence ineffective. Machine learning enhances anomaly detection, integrates threat intelligence across datasets, and supports predictive monitoring. In certain contexts, defensive automation significantly strengthens resilience. Nevertheless, these gains operate within a domain defined by comprehensive obligation. Defence must secure entire networks, ensure continuity of service, and minimise false positives that disrupt legitimate activity. Offence can concentrate on specific vulnerabilities, accept failure, and capitalise opportunistically on success. AI reduces the cost of opportunism more sharply than it reduces the burden of comprehensive protection.

The cumulative effect is a relative widening of offence–defence asymmetry in cyberspace. Both sides acquire enhanced tools, yet the structural characteristics of digital infrastructure enable offensive gains to translate more readily into scalable advantage. AI amplifies the selective logic of exploitation more effectively than it mitigates the systemic logic of protection.

The implications extend beyond technical cybersecurity. A perceived expansion of offensive advantage reshapes strategic incentives[169]. States that interpret increased vulnerability may invest more heavily in offensive cyber capabilities, anticipating the need for pre-emption or retaliation. The belief that AI-enabled intrusion is becoming easier can stimulate competitive dynamics even where defensive capabilities improve concurrently. As offensive operations become cheaper and more scalable, the threshold for initiating limited cyber actions may decline, rendering strategic interaction more fluid and potentially more volatile.

Artificial intelligence thus operates as a multiplier of pre-existing imbalance. It does not transform cyberspace into an entirely new strategic domain, nor does it negate defensive innovation. Rather, it alters the marginal calculus of effort in ways that deepen structural asymmetry. Appreciating this

[169] Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth' (2013) 38 *International Security* 41.

dynamic is essential for evaluating its broader consequences for escalation, deterrence, and strategic stability.

Section IV

Artificial Intelligence, Escalation Dynamics, and Strategic Stability

If artificial intelligence operates as an asymmetry multiplier in cyberspace, its relevance extends beyond questions of technical exposure. An imbalance between offence and defence matters because it reshapes strategic incentives. Classical security theory suggests that when offence is perceived to hold the advantage, actors experience greater pressure to adopt pre-emptive postures, to engage in competitive capability accumulation, and to interpret uncertainty as threatening. The effects are probabilistic rather than automatic: imbalance heightens the risk of instability. In the cyber domain, AI-induced shifts in relative advantage generate analogous concerns, albeit within a non-kinetic environment in which escalation manifests through disruption rather than territorial seizure.

Escalation in cyberspace differs in important respects from conventional military escalation. Cyber operations frequently remain below the threshold of armed conflict, encompassing espionage, intellectual property expropriation, infrastructure interference, and influence activities. Because such operations can be calibrated in intensity and obscured through ambiguous attribution, they enable incremental probing. Artificial intelligence reinforces this incremental dynamic by lowering the cost and increasing the speed of limited actions. As small-scale intrusions become cheaper to conduct, their frequency may increase, rendering strategic rivalry more persistent and less episodic.

A central concern lies in the compression of decision-making time. AI accelerates reconnaissance, exploit development, and adaptive evasion, thereby narrowing the window for detection and assessment. Defensive institutions may confront pressure to respond rapidly to ambiguous indicators[170]. In contexts where attribution remains uncertain, accelerated response elevates the risk of miscalculation. The conjunction of speed and uncertainty is inherently destabilising. Strategic stability depends in part on deliberation—the time required to evaluate intent, determine proportionality, and coordinate response. AI-driven acceleration reduces this temporal buffer.

At the same time, the destabilising implications of speed require careful qualification. Cyber operations rarely generate immediate physical destruction, and many are reversible or containable. This has led some observers to argue that cyberspace possesses stabilising characteristics, permitting signalling without catastrophic escalation. Artificial intelligence complicates this assessment in two respects. First, by enhancing scalability, it expands the potential magnitude of disruption. Second, by diffusing capability across a broader array of actors, it increases the number of potential sources of instability. Stability grounded in restraint among major powers becomes more fragile when non-state actors can initiate cascading effects.

---

[170] Joseph S Nye, 'Deterrence and Dissuasion in Cyberspace' (2017) 41 *International Security* 44.

Deterrence in cyberspace is already characterised by ambiguity. Effective retaliation depends upon credible attribution and proportionate response. If AI widens offence–defence asymmetry, it may weaken deterrence by reinforcing perceptions that defensive systems are increasingly penetrable. States that perceive persistent vulnerability in their critical infrastructure, despite defensive investment, may pursue alternative strategies, including forward defence or expanded offensive postures. Such approaches risk normalising sustained cyber engagement rather than confining competition to discrete episodes.

Perception plays a decisive role in this process. Offence–defence theory emphasises that actors respond not only to objective capabilities but also to perceived advantage. If policymakers interpret AI-enhanced cyber capabilities as decisively favouring offence, they may prioritise offensive development accordingly. This perception can generate competitive spirals even when defensive capabilities improve in parallel. The security dilemma intensifies when defensive research into vulnerabilities is indistinguishable from offensive preparation. AI amplifies this ambiguity, as similar machine learning techniques may underpin both intrusion and detection.

Threshold ambiguity further complicates escalation dynamics. In conventional deterrence theory, escalation thresholds are often associated with physical destruction or territorial violation. In cyberspace, such thresholds are less clearly defined. AI-enabled operations may permit increasingly intrusive or disruptive activity while remaining below established markers of armed conflict[171]. The cumulative effect of sustained low-level intrusions may erode trust and heighten suspicion without provoking overt retaliation. An environment of continual probing fosters strategic fatigue and reactive positioning.

It would, however, be analytically reductive to conclude that widening asymmetry necessarily produces instability. Defensive adaptation is ongoing. As AI-enabled attacks grow more sophisticated, defensive institutions may reorganise, introduce redundancy, and cultivate more resilient architectures. Strategic stability does not require invulnerability; it requires predictability and credible signalling. Should major powers develop shared norms regarding acceptable cyber conduct, AI-enhanced capabilities may be integrated into managed competition rather than uncontrolled escalation.

Yet the normative dimension remains underdeveloped. International agreements governing cyber operations are limited and frequently non-binding. The pace of AI development exceeds diplomatic consensus. In the absence of clearly articulated rules, states interpret one another's capabilities through worst-case assumptions, amplifying perceived imbalance. Uncertainty regarding AI's future trajectory—its autonomy, adaptability, and scalability—contributes to strategic anxiety.

An additional source of instability arises from the interaction between cyber and conventional domains. As digital systems underpin military command, logistics, and communications, AI enhanced cyber intrusion into these networks could affect crisis management. If states believe their command-and-control infrastructure is vulnerable to AI-driven disruption, they may perceive

[171] Miles Brundage and others, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Future of Humanity Institute 2018).

incentives to act early in crises rather than risk incapacitation. This logic echoes concerns from nuclear strategy regarding vulnerability and pre-emption, although the modalities and stakes differ.

AI's influence on strategic stability thus operates through multiple interconnected pathways: acceleration of operational tempo, diffusion of capability, amplification of perception-driven insecurity, and deeper integration of digital infrastructure with critical systems. None of these dynamics makes escalation inevitable[172]. Each, however, increases the complexity of deterrence and the difficulty of sustaining equilibrium.

A widening offence–defence asymmetry does not necessarily foreshadow catastrophic cyber conflict. Rather, it points toward a strategic environment characterised by persistent contestation, compressed response windows, and heightened suspicion. Artificial intelligence intensifies the structural conditions under which miscalculation becomes more probable, particularly when combined with ambiguous attribution and indeterminate thresholds.

Ultimately, the consequences of these developments depend not solely on technological innovation but also on political interpretation and institutional adaptation. Strategic stability in an AIenhanced cyber domain will hinge as much on norm development and governance as on technical capability. Nevertheless, if AI continues to reduce the marginal cost of offensive cyber operations more rapidly than it alleviates the systemic burden of defence, the underlying asymmetry will continue to exert pressure on established deterrence frameworks.

Section V

Rebalancing the Offence–Defence Equation in an AI-Enhanced Cyber Domain

If artificial intelligence deepens offence–defence asymmetry by lowering the marginal cost of offensive cyber operations more than that of systemic defence, then effective responses must address structural incentives rather than rely on isolated technical remedies. The challenge identified in this chapter is not merely the proliferation of AI-enabled threats, but the transformation of relative cost structures within cyberspace. Rebalancing therefore requires measures that raise the cost of offensive exploitation, reduce the burden of defensive maintenance, or recalibrate the strategic expectations that sustain competitive escalation.

The most foundational avenue of rebalancing lies in architectural reform. Cyberspace's offence bias is rooted in complexity and the retrospective addition of security to systems not designed with resilience as a primary objective. Artificial intelligence intensifies this condition by automating vulnerability discovery across expansive infrastructures. A structural response must therefore intervene at the design stage. Secure-by-design standards, mandatory code auditing, and liability regimes that sanction negligent software practices would elevate baseline security. By decreasing the density of exploitable vulnerabilities, such reforms increase the cost of offensive discovery

[172] Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press 2017).

even within an AI-augmented environment. The aim is not to eliminate vulnerability entirely, but to narrow the asymmetry generated by systemic fragility.

A second pathway involves redistributing the defensive burden. At present, defenders carry comprehensive responsibility for safeguarding complex networks, while attackers exploit isolated weaknesses. Collective defence mechanisms—shared threat intelligence platforms, synchronised patch management, and cross-sector response coordination—can reduce duplication and lower marginal defensive costs. AI-based detection systems perform more effectively when trained on aggregated datasets rather than siloed organisational logs. In this respect, cooperation functions as a defensive multiplier, counterbalancing the offensive multiplier effect produced by AI.

Yet technical coordination alone cannot rectify structural incentives. The persistence of asymmetry is reinforced by limitations in deterrence, particularly those stemming from attribution uncertainty. Improvements in forensic AI that enhance attribution reliability may strengthen deterrent credibility. Although perfect certainty is unattainable, reducing ambiguity alters strategic calculation. If offensive actors anticipate more consistent identification and coordinated response, the perceived cost of aggression increases. Enhanced attribution thus operates as an indirect mechanism for elevating offensive risk.

Legal and regulatory reform also has structural implications. Current market incentives in software production do not fully internalise security externalities. Clearer liability standards for severe security failures would shift costs from victims to producers, altering investment incentives. When firms face tangible repercussions for inadequate safeguards, preventive investment becomes economically rational. Over time, strengthened baseline resilience diminishes the exploitable surface available to AI-assisted reconnaissance.

International norm development addresses the perceptual dimension of asymmetry. Offence–defence theory underscores the influence of expectations on strategic behaviour. If states perceive AI-enhanced cyber capabilities as unconstrained and readily deployable, they are more likely to invest pre-emptively in offensive instruments. Norms delineating protected targets—such as critical civilian infrastructure—can stabilise expectations even amid technological change. While norms do not eliminate capability, they restrict its legitimate application, thereby moderating worst-case assumptions.

The governance of AI dissemination presents an additional structural consideration. Open distribution of advanced generative or code-producing models lowers expertise thresholds broadly, including for malicious actors. Conversely, excessive restriction may impede defensive innovation. A calibrated approach—incorporating safety testing, red-teaming protocols, and monitored deployment—can introduce friction against misuse without suppressing legitimate research. Such mechanisms moderate the pace at which offensive marginal costs decline.

Rebalancing does not necessitate the complete eradication of offensive advantage. In international politics, perfect equilibrium is rarely attainable. The objective is to prevent widening asymmetry from destabilising strategic expectations. Investments in resilience, redundancy, and rapid recovery capacity can diminish the strategic payoff of intrusion. Systems designed to degrade gradually rather than fail catastrophically reduce the expected benefit of attack, thereby lowering incentive even where technical penetration remains feasible.

Adaptation must also occur at the doctrinal level. Cyber defence should be integrated into comprehensive strategic planning rather than treated as a peripheral technical function. Clear articulation of red lines, proportional response frameworks, and escalation management mechanisms can mitigate ambiguity. As artificial intelligence compresses operational tempo, doctrine must compensate by clarifying response logic in advance. Predictable signalling reduces uncertainty and constrains escalation dynamics.

The central analytical insight is that AI-induced asymmetry is neither fixed nor inevitable. It arises from the interaction between technological capability and structural context. By reforming architecture, strengthening collective defence, enhancing attribution, realigning economic incentives, developing norms, and clarifying doctrine, actors can influence the trajectory of the offence–defence balance. Although the effectiveness of such measures will vary across political systems, their shared objective is to reshape relative marginal costs rather than merely respond to discrete threats. Rebalancing is therefore a process of structural adaptation. Artificial intelligence magnifies existing asymmetries; deliberate institutional innovation can mitigate that amplification. Whether such adaptation can keep pace with technological advancement remains uncertain. Absent structural intervention, however, the logic of asymmetry outlined in this chapter is likely to continue shaping the evolution of the cyber threat environment.

Conclusion

This chapter has examined whether artificial intelligence alters the offence–defence balance in cyberspace. Rather than approaching AI as a discrete technological breakthrough, the analysis has situated it within the enduring structural conditions that define the cyber domain. The central argument has been that cyberspace exhibited offence-leaning asymmetry prior to the diffusion of advanced AI systems, and that AI deepens this asymmetry by reducing the marginal cost of offensive action more substantially than it alleviates the systemic burden of defence. The structural baseline is therefore decisive. Digital infrastructures are complex, interdependent, and in constant evolution. Defenders carry comprehensive responsibility for securing systems in which vulnerabilities are statistically unavoidable. Attackers require only selective success. Attribution remains uncertain, deterrence constrained, and capability diffusion ongoing. Artificial intelligence enters this environment as a force multiplier. By automating reconnaissance, enabling scalable deception, accelerating adaptive exploitation, and lowering expertise thresholds, AI reinforces the selective logic of intrusion. Although defensive actors also benefit from automation, their gains are circumscribed by institutional constraints, reliability requirements, and the imperative of systemic continuity. The outcome is a widening of relative advantage rather than a balanced transformation. AI magnifies pre-existing imbalance because the underlying architecture of digital systems remains vulnerability-dense and economically misaligned. Rebalancing, therefore, does not entail suppressing AI development but reshaping the structural context within which it operates. Secure-by-design principles, collective defence coordination, improved attribution mechanisms, realigned economic liability, normative boundary-setting, and doctrinal clarification all operate upon the cost structures that underpin the offence–defence balance. By raising the expected cost or diminishing the anticipated payoff of offensive cyber operations, such measures can temper the asymmetry intensified by AI. The strategic trajectory of cyberspace will depend less on the intrinsic sophistication of AI systems than on the institutional adaptations that

accompany their integration. Offence–defence theory underscores the dynamic nature of balance: technological innovation may shift relative advantage, but governance, coordination, and perception can recalibrate it. Should states interpret AI-enhanced intrusion as an uncontested advantage and respond primarily through competitive offensive expansion, instability is likely to deepen. Conversely, if adaptation prioritises structural resilience and calibrated normative frameworks, asymmetry may be moderated even amid rapid technological change. Artificial intelligence does not convert cyberspace into an entirely new strategic arena. Rather, it sharpens and accelerates existing characteristics. It hastens processes that were previously slower, scales activities that were once limited, and diffuses capabilities that were formerly concentrated. Whether this sharpening results in sustained instability or in managed competition will depend on the extent to which political actors confront the structural foundations of imbalance rather than merely its technological expressions. The offence–defence balance in cyberspace is not a fixed conclusion but a continually evolving equation. AI has altered its variables. The eventual outcome will hinge on the effectiveness of institutional responses to that alteration.

----------**********----------

Chapter 9

State and Sovereignty in Cyber Space: Government Frameworks, Laws, and Security Tools

Aungshuman Ghosh, Advocate Supreme Court of India & Visiting Faculty Department of Legal Studies Swami Vivekananda University, Barrackpore, West Bengal.

Abstract

The emergence of cyberspace as a domain of geopolitical contestation has fundamentally disrupted conventional notions of territorial sovereignty and state authority. Unlike physical domains where boundaries are cartographically defined and legally recognized, cyberspace operates as a borderless, decentralized, and asymmetric environment — one in which the traditional Westphalian framework of state sovereignty faces its most formidable challenge yet. This chapter examines the intricate relationship between state power and cyberspace, interrogating how governments across the world have responded to the imperatives of digital governance through the development of legal frameworks, regulatory architectures, and technological security tools.

The chapter begins by deconstructing the myth that cyberspace exists beyond the reach of sovereign authority. While early internet discourse celebrated its emancipatory and ungovernable character, the reality of contemporary cyberspace reflects an increasingly fragmented landscape — one shaped by competing national interests, divergent regulatory philosophies, and the growing assertion of digital sovereignty by state actors. From China's "Great Firewall" and Russia's sovereign internet legislation to the European Union's General Data Protection Regulation (GDPR) and India's evolving data protection jurisprudence under the Digital Personal Data Protection Act, 2023, states have demonstrated both the will and the capacity to territorialize the digital domain.

Central to this analysis is a critical assessment of the international legal frameworks governing state conduct in cyberspace. The chapter evaluates the applicability of existing instruments of public international law — including the UN Charter, customary international law, and the Tallinn Manual 2.0 — to cyber operations, exposing significant normative gaps and interpretive ambiguities that states and non-state actors routinely exploit. The absence of a binding multilateral treaty on cybersecurity, combined with the attribution challenge inherent to cyber incidents, continues to undermine accountability and collective security in the digital realm.

The chapter further explores the domestic legal responses of key jurisdictions, analyzing how national cybersecurity laws, cybercrime legislation, and critical information infrastructure protection regimes function as instruments of both security and control.

Particular attention is given to the tension between state surveillance imperatives and the fundamental rights of citizens — a tension that legislation such as India's Information Technology Act, 2000 and its amendments, the United Kingdom's Investigatory Powers Act, 2016, and the United States'

Cybersecurity Information Sharing Act, 2015 have only partially resolved. The chapter argues that effective cybersecurity governance cannot be reduced to a technical exercise in deploying firewalls, encryption protocols, or intrusion detection systems; it is, at its core, a normative and institutional challenge demanding coherent legal architecture, inter-agency coordination, and meaningful democratic oversight.

The chapter concludes by proposing a multi-stakeholder model of cyber governance that reconciles state sovereignty with the transnational character of cyberspace. It advocates for enhanced international cooperation, capacity-building in developing nations, and the embedding of human rights principles within national cybersecurity strategies. Ultimately, the chapter contends that the myth of the impenetrable digital fortress — whether technological or legislative must yield to a more honest and resilient conception of cyber governance, one grounded in accountability, adaptability, and the rule of law.

Keywords: *Cyber Sovereignty, Digital Governance, Cybersecurity Law, International Law, Data Protection, State Surveillance, Critical Infrastructure, Cyber Warfare, Information Technology Act, Tallinn Manual.*

Key Outcomes

- Researching how state sovereignty developed through borderless cyberspace and digital domains shows its current state.
- The study examines international legal frameworks which control cyber operations to determine how these laws apply to state activities.
- The study analyzes domestic cybersecurity laws which exist in major jurisdictions such as India the United States the European Union and China.
- An examination involving the degree of state-security requirements that may infringe on fundamental human rights in cyberspace governance.
- An analysis into how security technologies or systems interact with prevailing legal and regulatory regimes.

Introduction: Sovereignty in the Digital Age

The concept of state sovereignty is rooted in the Westphalia Treaty (1648), which lays out a definition of sovereignty in terms of state action, which is made exclusive within its walls. The

classic concept of "sovereignty of the state"[173] holds that a country is supreme in terms of both the citizens and the inhabitants of the physical territory, undisturbed morally or physically from outside forces. In the cyberspace paradigm that has been introduced to undermine and alter the concept of territoriality, cyberspace is based on a network system that extends beyond physical boundaries and is devoted to global (data; aural, oral) communications. Specifically, the Internet has created great ambiguity in the manner people considered sovereignty when words like "sovereign"[174] evaporated, while some positions were creating questions about the probability of extant sovereignty structures ensuring some control over online operations, and there is a strong case for some urgency in considering novel structures of power and governance.[175] In the early years of the Internet, most discussions were full of a kind of techno-utopianism-a viewing of cyberspace as a wild, interstice, a digital common beyond the reach of any State, no matter how authoritative. From the "Declaration of the Independence of Cyberspace"[176] proposed by John Perry Barlow, came the idea that digital networks constitute an area that can slip outside the sovereignty of nation-states. That romantic viewpoint is totally prescription today on account of the stress these past twenty years have put on the governments. Basically, throughout the world governments have displayed both desire and ability regarding the employment of technology and law to capture the control over Cyberspace and to in fact disintegrate the once lofty dream of a worldwide digital network into a group of disjoined national online territories.[177]

Cyber sovereignty assertion has occurred through different methods which include technical infrastructure controls and legal frameworks and surveillance systems and international coordination efforts. China's internet filtering system and Russia's internet sovereignty system both demonstrate Cyber sovereignty through their operations.

Conceptualizing Cyber Sovereignty: Theoretical Foundations:

The Westphalian Challenge

In order from minor to major, the Westphalian concept of sovereignty is framed upon the notions of territorial integrity, political autonomy, and legal equality among independent states. None of these three can be realized in the digital domain. The constitution of digital territory presently finds itself taking a wholly digital-oriented form that comprises a pattern of meshed networks as well as sets of servers and data flows enforced by user information across different legal domains. In a very practical setting, an email will take just a couple of seconds to transmit from one server

---

[173] Arora, S. (2023). Digital Personal Data Protection Act, 2023: A critical analysis of exemptions and enforcement mechanisms. *Indian Journal of Law and Technology*, 19(2), 145-172.

[174] Ibid..

[175] Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24-42). National Defense University Press.

[176] Arora, S. (2023). Digital Personal Data Protection Act, 2023: A critical analysis of exemptions and enforcement mechanisms. Indian Journal of Law and Technology, 19(2), 145-172.

[177] Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

to another located in various places around the world, providing itself many entangled problems about which state has the right to monitor, control, regulate, etc., the transaction. [178]

The necessary algorithm for this process to make political independence challenging is to form a web with its infrastructure spreading throughout all systems. No state, on the grounds of a statewide economy, can ever completely become independent of cyberspace. There is an interface between national networks international protocols and domain name systems, while the physical cyber infrastructure functions from one legal territory to another. Thus, the internet control mechanism quite naturally works on simplistic lines as a multi-stakeholder system rather than being state-led to isolate internet resources and root servers and global routing systems. Such a mechanism virtually binds together all territorial statuses, hugely contrasting with the rights-ofsovereignty that are given to states on land.[179]

Third-party assessor discusses that the concept of Westphalian sovereignty of international equality is now diminishing due to technological disparities in cyber capabilities of different national states.[180] A plethora of technical capacities, its extensive know-how - whether about the good sophistication, security, offensive cyber warfare, and what have you-needed contribute considerably to the degree to which one of the countries is able to tag along, with the US and China or Russia of established giant cyber powers, or Israel running with high-tech cyber abilities, whereas the relatively low-cyber-capacities within individual member states could all be derived from the European Union. Some contrast to this, however, exists in the sense that most low-income countries lack even rudimentary cybersecurity measures. These differences in capability between countries mean that sometimes one country may just end up controlling another distant territory with the state remaining quite penetrable from beyond against international threats or internal, for that matter.[181]

Competing Models of Digital Governance

Two contrasting narratives are brought up currently around the very contemporary topic of cybersecurity. One points towards a liberal democracy-like model which offers a power- sharing platform in governance between many entities, be they governments, private sector, NGOs, and tech industry. The system could then be aligned like CSC group IANA or Internet Engineering Group around the three fundamental principles: public access; systems operability; and constraint of state power.[182]

Another model, the complete central authority or the government with some underlying authority, states that the cyberspace in any nation should come under the complete control of the state as if it were an indispensable part of the territory, with no scope for trade-off on grounds of national security or police integration and internet censorship. China's argument on "cyber sovereignty"[183]

---

[178] Brenner, S. W. (2007). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology*, 97(2), 379- 475.

[179] Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

[180] Ibid.

[181] Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

[182] DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

[183] DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press

is probably the most complete implementation of such a model. According to the statement of the government of China, countries as states are entitled, and in the matter of policy commitment, obligated to manage their Internet intern systems in compliance with national laws and culture, while there is an added dimension that sees criticism from outsiders as an intrusion into sovereign rights.[184] The European Union develops its third model which establishes a system for government control that protects rights through its strong legal frameworks which govern both state and private sector operations. The General Data Protection Regulation (GDPR) serves as a regulatory sovereignty example because it enables EU legal standards to reach worldwide through its global enforcement power. The EU governance model requires effective control systems which include strong legal frameworks to limit state surveillance and corporate data operations while ensuring democratic oversight and fundamental rights protection.[185]

Table 1: Comparative Models of Cyber Governance

Governance Model	**Primary Actors**	**Key Principles**	**Representative Examples**
Multi-stakeholder	States, Private Sector, Civil Society, Technical Community	Openness, Minimal Intervention, Distributed Authority	ICANN, Internet Governance Forum, Early Internet Architecture
State-Centric Sovereignty	National Governments	Territorial Control, Regulatory Authority, Security Primacy	China's Great Firewall, Russia's Sovereign Internet Law, Iranian National Network
Regulatory Sovereignty	State Institutions with Rights Constraints	Legal Frameworks, Rights Protection, Democratic Accountability	EU GDPR, German NetzDG, French Data Protection Authority
Hybrid	Mixed State and	Pragmatic Balance,	India's IT Act, UK
Models	Private Coordination	National Security with Limited Openness	Investigatory Powers Act, Singapore Cybersecurity Act

[184] Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107- 145). Rowman & Littlefield.
[185] Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

International Legal Frameworks: Norms, Gaps, and Ambiguities:

Applicability of Public International Law to Cyberspace

Scholars and policymakers have ongoing discussions about how existing public international law applies to activities in cyberspace. The United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security reached its 2013 and 2015 conclusions about state behavior in cyberspace by stating that international law, together with the UN Charter, governs state activities in cyberspace. The agreement established a major achievement because it proved that states cannot treat cyberspace as an area without laws which protects them from their duty to follow international treaties.[186]

International law applicability remains an area now needing further attention. It does nothing to help with the ultimate question as to how legal rules become applied to cyberspace. The example of using force rendered illegal by the UN Charter, under Article 2(4), brings to light the difficulties of interpreting that signal. This prohibition is meant to prohibit kinetic military operations, but creates limitless uncertainties when applied to cyber operations. So, should a more active breakdown in the functionality of critical infrastructure achieved by a distributed denial-of-service cyber attack be considered as a use of force? Likewise, what about cyberspying, for instance by foreign intelligence agencies, wherever large-scale operation is concerned? On these questions, States are significantly divided, largely because of broader consensus as to where the threshold should be when assessing cyber activities as violations of sovereignty or acts of aggression.[187]

Test your understanding: In what way did poetry advance your understanding of love, death, or history in War of the Physicians? Stick to three examples from case materials supportive of your opinion, duly accepted by the community.

The Tallinn Manual Framework

There is no longer to wait to embellish the desktop with fascinating wallpapers by exploring your photographic abilities. By now, your picture frames are quite packed, but they prove inadequate. Even though unemployment forms are discussed by people, usually the hard-core job seekers fare well with handwriting superficial questions on resumes, the just conditions for face-to-face interviews vanish, and there is excessive weight on the question of what a person did.[188] However, by recording their portfolios online, several job seekers are entitling their fates to companies to evaluate their applications seriously through the information they supply directly. In terms of time, the concept should start with shots so less saleable they do not want them; [uploaders] may well have kept these images to this moment. Although the authors of the first

---

[186] Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy Institute Brief*, November 2017, 1-8.

[187] Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

[188] Ibid.

paragraph point to endorsements of the Tallinn Manual, the text originated from an academic study conducted with no government intervention. This study was built on expert opinions rather than on established international practice. Such study has not been based on actual international customary law or an ensuing legal doctrine. Its judgment on contested issues such as: the point at which a cyber operation will be characterized as a use of force or as an infringement on sovereign rights is accepted but not uniformly accepted as a legal principle.[189] Though the Manual has policy relevance, it does not serve as an effective tool for understanding state behavior in cyberspace because there remains no among legal experts about what a given legal definition.

Domestic Legal Responses: National Cybersecurity Frameworks:

The Indian Framework: Information Technology Act and Beyond

India's cyberspace legal system developed significantly from 2000 because of the Information Technology Act implementation. The IT Act enables electronic commerce through digital transaction recognition which later required legal amendments to solve new cybersecurity threats and cybercrime issues and content management requirements. The 2008 amendments created new laws which addressed cyber terrorism and data protection and set intermediary liability standards because the government had started to view cyberspace as a legal area that needed complete control.[190]

The IT Act center section 69 gives central and state governments special rights to monitor and intercept all information which people send through computer systems to protect national security and public safety and international relations and territorial integrity. Civil rights defenders have raised major privacy issues about government monitoring systems because these systems depend on special rules which the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 establish for monitoring and protecting information.[191] (Bhatia, 2019).

The Digital Personal Data Protection Act 2023 stands as India's current attempt to create a complete framework for data protection rights. The Act establishes three data protection principles which require data minimization and purpose limitation and individual consent in addition to establishing the Data Protection Board as the nation's data protection authority. The Act imposes major restrictions on government surveillance activities because its main exemptions allow security agencies to operate without restrictions when they conduct operations for national security or public safety or territorial integrity. The government has chosen to protect

---

[189] Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
[190] Maini, T. S. (2012). The Information Technology Act, 2000: A legal framework for cyber law in India. *Indian Journal of Law and Technology*, 8(1), 89-112.
[191] Bhatia, R. (2019). Surveillance, privacy, and the Information Technology Act: Examining Section 69 and procedural safeguards. *Journal of Indian Law and Society*, 10(1), 34-58.

national security and maintain flexible control over operations instead of protecting user privacy through this system of exemptions which has resulted in privacy complaints from users.

The United States Approach: Fragmented Regulation

The United States lacks a comprehensive federal cybersecurity law which matches the cybersecurity systems that other major jurisdictions have implemented. American cyber governance functions through a broken system which consists of specific industry rules and executive directives and optional security partnerships between public and private sectors. The Cybersecurity Information Sharing Act (CISA) of 2015 represents one of the few cross- sectoral federal initiatives which enable private companies and government bodies to exchange cybersecurity threat data. CISA fails to function as an all-encompassing governance instrument because its implementation depends on voluntary participation and the law provides only minimal liability coverage according to Watters.

Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience designates sixteen critical infrastructure sectors and establishes a framework for protecting these sectors from cyber threats through coordination between sector-specific agencies and private sector partners. The public-private partnership model serves as the American market- driven solution which requires minimal regulatory oversight while creating a stark contrast to standard regulatory methods that other jurisdictions employ. The Federal Information Security Modernization Act (FISMA) governs cybersecurity for federal agencies which need to do continuous monitoring and annual assessments and follow standardized security controls that use National Institute of Standards and Technology (NIST) guidelines.[192]

The Fourth Amendment of the United States Constitution protects citizens from government surveillance through its prohibition of unreasonable searches and seizures yet the extent of these protections remains disputed in relation to online activities. The Foreign Intelligence Surveillance Act (FISA) establishes procedures for electronic surveillance and physical searches related to foreign intelligence gathering while Section 702 of the FISA Amendments Act authorizes warrantless surveillance of non-U.[193]

The European Union: Rights-Based Regulatory Sovereignty

The European Union currently leads worldwide rights-based cyber governance because it developed extensive legal systems which regulate online activities while safeguarding essential human rights. The General Data Protection Regulation (GDPR), which entered into force in 2018, establishes stringent requirements for data processing, including principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. The GDPR applies extraterritoriality because it governs all

[192] Paganini, P. (2018). The evolution of U.S. federal cybersecurity policy: From FISMA to continuous monitoring. *International Journal of Cyber Warfare and Terrorism*, 8(3), 45-67.
[193] Ibid.

organizations that handle personal data from EU residents, which extends European Union legal standards throughout the world according to Bradford.[194]

The Network and Information Security (NIS) Directive, adopted in 2016 and updated as NIS2 in 2022, establishes cybersecurity requirements for operators of essential services and digital service providers. The directive requires member states to designate competent authorities, establish computer security incident response teams (CSIRTs), and implement national strategies for network and information security. The 2019 Cybersecurity Framework Act of the European Union gives EU Cybersecurity Agency (ENISA) added powers in setting up a European Certification Framework for cybersecurity-certification schemes. Certification guarantees that ICT products, services, and processes satisfy certain security requirements for trustworthiness and integrity of the single market where applicable. The legislation is the EU's endeavor to use regulation to shape security standards worldwide and extend influence.

China's Comprehensive Control Architecture

The Chinese government has established its cyber sovereignty system which functions as the most advanced system for state control over online activities through its comprehensive digital presence.

The Chinese Cybersecurity Law which became effective in 2017 requires network operators to implement security measures which include conducting security assessments and storing data within national borders and working with government intelligence agencies and security organizations. The law defines critical information infrastructure as essential systems which protect approximately 80 percent of China's digital economy from security threats through government monitoring.[195] The Chinese government uses its cybersecurity framework to implement multiple regulatory systems which include monitoring online content and monitoring social credit systems and conducting full-scale surveillance operations. The Great Firewall functions as an advanced system which uses technical filtering methods and DNS manipulation techniques and deep packet inspection methods to prevent users from accessing foreign websites and services which the government considers dangerous for national security and public order. Social media platforms in the country must enforce strict content control measures which create heavy legal liability for them if they do not delete banned materials without delay. The Chinese government uses advanced technological systems for social control through its implementation of artificial intelligence and big data surveillance technologies which operate in Xinjiang and other areas.[196]

The Data Security Law and Personal Information Protection Law establish the complete legal structure which governs China's digital operations through their 2021 enactment. The laws create a framework for data classification which establishes rules for cross-border data transfers and

---

[194] Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.
[195] Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107- 145). Rowman & Littlefield.
[196] Mozur, P. (2019). One month, 500,000 face scans: How China is using AI to profile a minority. *The New York Times*, April 14, 2019.

specifies conditions under which government authorities can access information stored by private companies.[197]

The framework shows China's intention to treat data as a national resource which the government will control while giving precedence to state security needs above individual and business rights. The current strategy uses data.

Table 2: Comparative National Cybersecurity Frameworks

Jurisdiction	Primary Legislation	Governance Approach	Key Features
India	IT Act 2000 (amended), Digital Personal Data Protection Act 2023	Centralized with security emphasis	Government interception powers, intermediary liability, broad security exemptions, emerging data protection
United States	CISA 2015, FISMA, Sector-specific regulations	Fragmented, public-private partnerships	Voluntary information sharing, critical infrastructure protection, Fourth Amendment constraints, sector-based regulation
European Union	GDPR 2018, NIS Directive/NIS2, Cybersecurity Act	Rights-based regulatory sovereignty	Extraterritorial application, comprehensive data protection, mandatory breach notification, certification schemes
China	Cybersecurity Law 2017, Data Security Law 2021, Personal Information Protection Law 2021	Comprehensive state control	Data localization, critical infrastructure security, content control, government access
			requirements, social credit integration
United Kingdom	Investigatory Powers Act 2016, Data Protection Act 2018, Network and Information Systems Regulations 2018	Balanced security and rights (post-Brexit hybrid)	Bulk interception powers, judicial authorization, incident reporting, GDPR adequacy maintenance

[197] Mozur, P. (2019). One month, 500,000 face scans: How China is using AI to profile a minority. *The New York Times*, April 14, 2019.

Security Tools and Technological Governance:

Technical Infrastructure and Control Mechanisms

The sovereignty of states to control their cyberspace depends on their capabilities to secure networks and manage their technology systems. States establish a framework of digital activity monitoring which includes technological systems that enable them to observe and control their online operations. The system provides two types of monitoring systems, with one being the lawful interception interface, which telecommunications networks must use and the other being advanced surveillance systems, which operate without public knowledge and democratic control.[198]

China's Great Firewall uses network filtering systems, which combine multiple technical strategies, including IP address blocking, DNS filtering, and redirection, URL filtering, and packet inspection, together with connection reset. States use these systems to block access to international websites and online services, while permitting users to connect to local services. Different jurisdictions show various degrees of technical development for these systems, as some countries use simple blocking methods, which users can bypass, while other countries use deep packet inspection and machine learning systems, which can detect and block encrypted data together with its circumvention tools.

Countries such as the United States, India, Australia, Spain, and the United Kingdom passed laws that enacted Telecommunications Assistance for Law Enforcement or CALEA to make telecommunications service providers build a system capable of lawful interception for government surveillance.[199] However, such countries had put certain regulations to incentivize end-to-end encryption and banned unnoticed crypto, condemned attempts to weaken any network design, or innovations for government.

Cyber Defense and Critical Infrastructure Protection

In the case of national cybersecurity strategies, attention to the protection of critical infrastructure as topically represented is now seeing several cyberattacks threatening the likes of all digital systems that support energy distribution, critical telecommunications networks, financial systems, water supplies, ground transportation infrastructures, and healthcare systems. Providing for the shortening of regulatory frameworks, the states have imposed baseline security measures, a requirement for incident reporting, and the provision for information sharing among privatesector operators in collaboration with government agencies.[200]

---

[198] Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, 21(4), 43-57.
[199] Ibid.
[200] Lewis, J. A. (2019). *Critical Infrastructure Protection and Cyber Resilience*. Center for Strategic and International Studies.

The elegance of the Cybersecurity Framework from the National Institute of Standards and Technology in the United States is a voluntary scheme that has been launched to voluntarily moderate the efforts to combat cybersecurity risks for critical infrastructure. It is based on the classification of its cybersecurity activities into five core functions: Identification, Protect, Detect, Response, and Recovery. It remains the most dominant standard in most sectors, while on a voluntary basis, because the standard asserts standardization presentations that are beneficial in business ventures involving large installations, exercising joint acceptance of them.[201] So, some concerted endeavor is most pressing for the intention to make possible the most viable arrangement of technical, procedural, and control mechanisms guaranteeing a likely assurance against intrusion vectors, devoid of a cumbersome, overly stringent tigress of imminent regulation that would be rendered obsolete too hastily by rapidly changing technology behaviors.

Having the Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) solve cybersecurity incidents also resulted in working with the national and sector teams that are a part of these consortia. National CERTs operate in most countries to manage cyber incidents through their response coordination, threat intelligence sharing, and technical aid provision to government bodies and critical infrastructure operators. International coordination among CERTs through forums such as FIRST (Forum of Incident Response and Security Teams) enables international collabouration to combat cyber threats because effective cyber defense needs both national capabilities and international partnerships.[202]

The Surveillance-Rights Tension: Democratic Accountability in Cyber Governance

The declaration of state control over cyberspace leads to conflicts between security needs and essential human rights which include privacy rights and freedom of speech and the right to fair legal proceedings. Democracy requires security systems to function within established constitutional boundaries which demand proper supervision and which should only be used for genuine government needs. The combination of complex technical systems for cyber surveillance together with hidden intelligence work and ineffective control systems prevents organizations from achieving their accountability standards according to Diffie and Landau.[203]

The Edward Snowden disclosures from 2013 revealed how the United States National Security Agency and its partner intelligence agencies operated extensive and sophisticated surveillance programs. The programs conducted bulk telephone metadata collection which enabled them to intercept internet traffic through their partnerships with telecommunications companies and they used commercial encryption system weaknesses to conduct their operations. The revelations created a global scandal which led to multiple countries implementing changes including USA FREEDOM Act in the United States and legal actions that resulted in the Schrems II decision by

[201] Ibid.
[202] Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42-57.
[203] Diffie, W., & Landau, S. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press.

the European Court of Justice which rendered the EU US Privacy Shield agreement invalid according to Greenwald 2014.[204]

To achieve proper democratic control over cyber surveillance, multiple institutional structures need to be established. First, democratic legitimacy requires legal authorization through legislation instead of using executive power to establish limits on discretionary authority. Second, judicial oversight needs to include specific requirements for individualized warrants which must meet the probable cause standard or an equivalent threshold, to prevent unauthorized surveillance. Third, all organizations need to meet legal security requirements when disclosing their surveillance activities and operations according to defined requirements.

Toward a Multi-Stakeholder Model: Reconciling Sovereignty with Transnational Governance

The existing conflict between territorial sovereignty and cyberspace's transnational nature needs more than state actions and technical solutions to achieve its resolution. Cyber governance requires multiple stakeholders to work together because states and international organizations and private sector entities and civil society organizations and technical communities need to cooperate. Stakeholders in governance frameworks possess separate abilities and requirements and viewpoints which need to be unified.[205]

Certainly, there are significant political DPI issues in international cybersecurity cooperation.

Antagonism among the great powers turned on fundamental differences over norms governing the behavior of states in cyberspace, with authoritarian regimes speaking of state sovereignty and content control, while liberal democracies argue for openness and fundamental rights. At the international level, cybersecurity endeavor could not proceed, due to an irreconcilable normative position between two Chinese and Russian proposal for an International Code of Conduct for Information Security and the Western countries taking up the United Nation Group of Governmental Experts (UN GGE) meeting process which was to frame a voluntary, agreed-upon set of norms.[206]

Operational partnerships offer proof positively that cybersecurity cooperation has succeeded, in the face of the political impediments. Intergovernmental cooperation targeting the implementation of law enforcement in transnational cybercrime, inter alia, with Interpol cybercrime programs and mutual legal assistance frameworks, remains a possibility. ICANN and Internet Engineering Task Force (IETF) and the regional internet registries are technical bodies for coordination, which, through their capabilities of operational coordination, maintain the global internet infrastructure.[207] It thus may be observed that effective cyber governance is

---

[204] Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.
[205] DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
[206] Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy*
[207] Watters, P. (2016). The Cybersecurity Information Sharing Act: A legislative response to cyber threat proliferation. *Georgetown Journal of International Affairs*, 17(3), 125-138.

security-held by a formal operational partnership of an international nature, rather than the great many multilateral agreements.

Conclusion

The developing international system in cyberspace shifts the compartments. It is simply untenable to propose that cyberspace is ungovernable and therefore free from sovereignty. States have increasingly asserted their will to exert control over digital networks and thus raise legal and technological mechanisms and regulatory architectures that position the space closer to the national interest and political system; thus, governance systems across jurisdictions have a range of effectiveness and legitimacy, depending on their operational standpoint and doctrinal inconsistency. Based on many widely accepted international norms, domestic forces may thus be useful in providing such guidelines for the behavior of states in cyberspace, with many needs to fill gaps and resolve ambiguities in frames of reference of rights regarding the "non-usage" of borders.[208] Public international law, a term preferred by many supportive professors, is claimed to govern cyberspace operations everywhere while details such as points of threshold and proportionality in attribution raise yet more complex questions, not to mention the policy questions of how to respond to incidents. The increasingly frequent collusion that states mount in the grey areas operating less than formal legal limits makes it difficult for everyone to anticipate the behavior of the said nations or for resulting actions to subsequently be condemned by the accepted norms of international law. Variably different domestic legal frameworks create varied governance models-some riotous,

while others would be bordering on regulatory sovereignty or semi-principle-based regulatory sovereignty; where they seek a balance between state authority and private sector participation in various ways, each one putting the security vs rights argument first and then the economic efficiency vs equal access- to-innovation one.

The second concept (that is, equal access for all) runs parallel to the idea of ensuring all rights for all people and places; to what safeguards will the governance apparatus subscribe at the price of other rights? Vigorous debate about surveillance versus rights would now set out greener and more incipient paths that are not-and indeed never will be-hatch for established regulatory bodies. Thus, accounting for probable restraining conditions on surveillance by state institutions does require intense democratic oversight specimens accompanying judicial review and compliance with transparency demands on independent data protection.

----------**********----------

[208] Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy*

Chapter 10
Plagiarism and Cybersecurity in the Digital Age: A Cross-Level Study of Academic Integrity in Higher Education

Dr. Richa Chaurasia, Assistant Professor & Head, Department of Education, Saheed Anurup Chandra Mahavidyalaya, University of Calcutta

Abstract

Plagiarism has evolved significantly in the digital age, transforming from traditional cut, copy and paste based misconduct to technologically facilitated academic dishonesty. Simultaneously, cybersecurity threats in higher education institutions have intensified and alarming, at the same time exposing vulnerabilities related to intellectual property theft, unauthorized data access, and digital manipulation of academic manuscripts and content. The present study examines the intersection of plagiarism and cybersecurity across and among undergraduate (UG), postgraduate (PG), doctoral (PhD), and faculty levels. A cross-sectional survey of 200 participants was conducted to assess awareness, attitudes, experiences and expectations related to plagiarism and institutional cybersecurity mechanisms. The findings reveal high dependence on digital sources, moderate awareness of plagiarism policies, and limited understanding of cybersecurity frameworks about protecting academic data. Results indicate a statistically significant relationship between usage of digital tool and unintentional plagiarism practices. The study concludes that plagiarism must be addressed prominently as an ethical issue and also as a cybersecurity concern requiring technological, institutional, and behavioural interventions.

Keywords: *Plagiarism, Cybersecurity, Academic Integrity, Digital Ethics, Intellectual Property, Ethical Issues.*

Introduction

Plagiarism is traditionally defined as the act of presenting another individual's intellectual work ideas, words, data, or creative expressions as one's own without proper acknowledgment. Historically, plagiarism was confined to manual reproduction of texts. However, the rapid expansion of internet accessibility, cloud storage systems, and artificial intelligence tools has fundamentally transformed its scale and complexity. Higher education institutions increasingly rely on digital platforms for teaching, submission of assignments, peer collabouration, and research dissemination. While these advancements have democratized knowledge, they have also created opportunities for academic misconduct. Digital plagiarism now includes copy-paste practices, paraphrasing software misuse, AI-generated text submission, and code replication.

At the same time, universities face escalating cybersecurity threats. Data breaches, ransomware attacks, unauthorized database access, and intellectual property theft threaten academic ecosystems. The intersection between plagiarism and cybersecurity emerges when research data, unpublished theses, or proprietary academic content are accessed or misused through digital vulnerabilities.

Plagiarism is no longer solely an ethical violation; it has become intertwined with digital security frameworks. Understanding this intersection is essential across UG, PG, and PhD levels, as well as among faculty who guide research integrity.[209]

This study aims to:

1. Examine the evolving nature of plagiarism in the digital environments.
2. Analyse cybersecurity and vulnerabilities that facilitate academic misconduct.
3. Assess awareness levels of students and faculty across UG, PG and PhD.
4. Provide recommendations based on evidence for strengthening academic integrity systems.

Review of Related Literature:

- Evolution of Plagiarism in Digital Contexts

1. Research indicates that internet proliferation has significantly increased plagiarism rates among students. Digital accessibility reduces the perceived effort required to replicate academic material. Studies show that students often engage in unintentional plagiarism due to inadequate citation knowledge.[210]

2. AI-based writing systems have further complicated detection mechanisms. Automated content generation tools blur the boundary between assistance and misconduct, challenging traditional definitions of originality.

- Cybersecurity in Higher Education

1. Universities hold large volumes of sensitive data such as unpublished research, patents, examination systems, and personal student records. According to cybersecurity frameworks proposed by the National Institute of Standards and Technology (NIST), US based standards agency that academic institutions often lack enterprise-level security infrastructure.[194]
2. Research published by IEEE organisation professional association for technology emphasizes the growing trend of ransomware attacks targeting educational institutions.

[209] Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

[210] Bretag, T. (2016). Challenges in addressing plagiarism in education. Educational Integrity Journal, 12(2), 45–59.

These attacks not only disrupt operations but also expose confidential academic material.[211]

- Detection Tools and Technological Safeguards

1. Plagiarism detection services such as Turnitin use similarity indexing and algorithmic comparison to detect content overlap.[212] However, these systems primarily address textual similarity rather than cybersecurity vulnerabilities like unauthorized file access.[213]

2. Studies suggest that integration of blockchain technology could secure academic authorship records and timestamp intellectual property.[214]

Although plagiarism and cybersecurity have been individually studied by a large number of researchers but limited empirical research explores their intersection across academic levels. Therefore, the present study bridges that gap by combining theoretical analysis with survey-based evidence.

Theoretical background of Plagiarism and Cyber security

1. Deterrence Theory

Deterrence theory suggests individuals are less likely to commit misconduct when the perceived risk of detection and punishment is high. Plagiarism detection software acts as a deterrent mechanism. However, if the cybersecurity systems are weak there is a high opportunity of increase in misconduct.

2. Routine Activity Theory (Cyber Adaptation)

This theory posits that in digital academia crime occurs when three elements converge. They are: -

The blockchain and kudos: A distributed system for educational record.
Journal of Learning Analytics, 3(3), 1–7.

- Motivated offender i.e. student or researcher,
- Suitable target i.e. digital academic content

---

[211] Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

[212] Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

[213] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity.

[214] Bandhopadhya, A.K. (2008). *International Encyclopedia of Audio Visual Media (Vol- 1)*Delhi: Anmol Publication Pvt Ltd

- Absence of capable guardian i.e. cybersecurity & plagiarism systems[1]

The study concludes that weak digital guardianship increases risk of crime or misconduct.

3. Technology Acceptance Model (TAM)

TAM explains that perceived usefulness and ease of use influence adoption of detection software. Faculty acceptance significantly impacts institutional enforcement of plagiarism policies.

The study is based on following methodologies.

i) Research Design- A quantitative cross-sectional survey was conducted.

ii) Population – The population of the study will consist all the undergraduate students, post-graduate students, research scholars and faculty members of University of Calcutta and its affiliated colleges.[215]

iv) Sample - There are 100 participants as shown in detail in the table below which are selected from the population.[216]

Sl. No.	Types of participants	No. of participants
1	Undergraduate	40
2	Post- graduates	25
3	Research Scholars	20
4	Faculty Members	15
Total no. of participants		100

iii) Sampling Method

Convenience sampling method within the university setting is employed here.

iv) Tool

[215] Ibid.

[216] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity.

A self- made structured questionnaire containing short answer type, one word answer type, MCQ type and Yes or No type items constructed and administrated. The detailed structure of questions is given in the table below.

Sl. No.	Types of questions	No. of questions
1	Demographic questions	5
2	Likert-scale questions	15
3	Yes/No questions	5
Total no. of questions		25

v) Ethical Considerations

The study is conducted in an open environment where voluntary participation is encouraged and anonymity of the participants are maintained. However, the data collected strictly used for academic research only.

Data Analysis

The data collected are analysed through Descriptive statistics i.e. percentage analysis and Correlation analysis among the students, research scholars and faculty members based on three main points. They are - - Digital tool use

- Plagiarism awareness

- Cybersecurity awareness

Results of the Survey

- Demographic Distribution

Sl. No.	Category of participants	Percentage of participants
1	Undergraduate	40%
2	Post- graduates	25%
3	Research Scholars	20%
4	Faculty Members	15%
TOTAL		100%

Findings of the study-

The key findings of the study are mentioned as follows.

A. Study of awareness of plagiarism policy: 78% of participants have keen awareness where 22% are partially aware.

B. Study of awareness of Cybersecurity Policy: 46% of participants are aware where 54% are unaware.[217]

C. Use of online sources without proper citation: 72% of participants uses online sources without proper citation and 18% of participants frequently omits where 10% never use any.

D. Use of AI tools: 64% of participants reported using AI assistance frequently among them undergraduate students have higher usage of 82%.[218]

E. Study of Confidence in Detection Tools: - 58% of participants have moderate confidence, 25% have high confidence and 17% low confidence.

Correlation Finding

A moderate positive correlation (r = .52) was observed between heavy digital tool usage and selfreported unintentional plagiarism.

Discussion

- The findings of the study suggest that while plagiarism awareness is relatively high among all whereas cybersecurity awareness remains significantly lower. This gap exposes institutions towards academic misconduct facilitated through digital systems.
- Undergraduate students show higher AI tool usage. Hence potentially increasing unintentional plagiarism risk among them.
- Faculty members show high confidence in detection systems that suggests institutional trust, yet awareness gaps among students weaken preventive impact too.

---

[217] Becta, (2004) British Educational Communications and Technology Agency. *A review of the Research literature on barriers to the uptake of ICT by teachers*

[218] Jain, M.E. and Agarwal, J.C. (2008) *Encyclopedia of Education (Vol-2)* Delhi: Anshan publishing house

- The moderate correlation between digital tool use and plagiarism indicates that technology, without structured guidance, increases vulnerability.[219]

Recommendations

1. There must be mandatory cybersecurity and academic integrity training in all levels of higher educational institutes for both students and faculties.
2. The integration of plagiarism detection into Learning Management Systems.
3. Introduction of Blockchain timestamping of theses and study materials.
4. There must be Two-factor authentication for academic submissions.
5. National academic cybersecurity frameworks should be developed.
6. AI-detection algorithm should be upgraded.

Conclusion

Therefore, it can be concluded that plagiarism in the digital era extends beyond the ethical misconduct and misuse. Hence, intersects with institutional cybersecurity vulnerabilities. In spite of availability of numerous detection tools, awareness and technological safeguards remain uneven across all academic levels both among students and teachers. Therefore, institutions must adopt a holistic strategy by combining education, technology and policy enforcement to protect intellectual integrity and minimise misconduct.

Suggestion for further studies

The present study has been conducted on a sample of students and teachers in the city Kolkata. This study may be replicated on school students and teachers and students and teachers of urban and rural areas, students and teachers of English medium as well as Hindi medium at different levels of education with different Boards of education. Studies may also be conducted to find out interaction or comparison between students and teachers of different universities, colleges or streams.[220]

----------**********----------

[219] Anandan,K. & William Dharma Rja, B. (2010). *Educational Technology,* New Delhi: A.P.H. Publishing Corporation

[220] IEEE. (2020). Cybersecurity threats in higher education institutions. IEEE Security Review, 18(4), 22–30.

Chapter 11

Constitutionalism and Cyberspace Governance

Susmita Ghosh, Assistant Professor (Law), Swami Vivekananda University

Abstract

The expansion of digital technologies has fundamentally transformed the architecture of state power, raising critical questions about the applicability and resilience of constitutional principles in cyberspace governance. As governments increasingly rely on digital infrastructures for surveillance, data collection, cybersecurity, and public administration, the traditional understanding of constitutionalism - limited government, rule of law, separation of powers, and protection of fundamental rights- faces unprecedented challenges. Cyberspace operates across borders, often through algorithmic and automated systems, complicating established doctrines of territorial jurisdiction, accountability, and transparency. This chapter examines how constitutionalism adapts to digital governance, focusing on privacy, surveillance, data protection, intermediary regulation, and algorithmic decision-making. It analyses the recognition of informational privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India, which articulated the proportionality test as a constitutional standard for assessing state interference in digital contexts. The chapter further explores how statutory frameworks such as the Digital Personal Data Protection Act, 2023 seek to operationalize constitutional safeguards, while also raising concerns regarding state exemptions and oversight mechanisms. Comparative reference is made to the General Data Protection Regulation, which emphasizes accountability, data minimization, and individual autonomy.

The chapter argues that constitutionalism in cyberspace must evolve beyond traditional models to incorporate digital due process, algorithmic transparency, and robust judicial review. Courts play a crucial role in ensuring that technological governance remains subject to legality, necessity, and proportionality. Ultimately, the future of democratic governance depends on embedding constitutional values within digital infrastructures to prevent the normalization of unchecked surveillance and algorithmic control. Cyberspace, far from existing outside constitutional order, represents a new frontier where constitutional guarantees must be reaffirmed and reimagined.

Keywords: *Cyberspace, Digital Due Process*, *Data Minimization, And Individual Autonomy.*

Introduction

Constitutionalism is a foundational political philosophy that governs the relationship between authority and individual rights through a constitution. Constitutionalism requires that all state actions are to be done within the limits of law by establishing the principles and framework of law that limit the power of the government.

The rapid development of digital technologies has essentially transformed the structure of the governance and relationship between the citizens and state. Governments today rely extensively on digital infrastructures for administration, public service delivery, national security, and regulation of

the social and economic activities. Cyberspace has therefore emerged as an important domain of governance where political authority, legal norms, and technological systems intersect.[221]

The constitutional frameworks were outlined at the time when administration was executed through territorial institutions and physical state machinery. The proliferation of AI, emergence of data driven and global communication platforms has fundamentally reshaped the traditional exercise of state power. The modern authorities are exercising unparalleled power to track communications, harvest personal data, and regulate digital spaces. This can also create threats to individual rights and democratic freedoms.

Constitutionalism, which emphasizes the limitation of governmental authority through the rule of law and protection of fundamental rights, plays a very important role in addressing these challenges. The principles of constitutional governance ensure that state actions remain accountable, transparent, and consistent with democratic values. In the digital era, constitutionalism must adapt to regulate new forms of power exercised through digital technologies.[222]

In contemporary constitutional jurisprudence the recognition of digital rights is an important aspect. Judiciary around the world recognize fundamental rights including privacy and freedom of speech and apply it to the digital world. By following this trend, the Indian Supreme Court in Justice ***K.S. Puttaswamy (Retd.) v. Union of India***[223] affirmed that right to privacy is a fundamental constitutional right and is a legal foundation for protecting digital autonomy and personal data.

Fundamental Rights in Cyberspace

The expansion of digital technologies has significantly influenced the scope and interpretation of fundamental rights. Rights that were traditionally exercised in physical spaces now operate within digital environments. The internet has become an essential platform for communication, political participation, economic activity, and social interaction.

One of the most important constitutional developments in this context is the recognition of the right to privacy in the digital sphere. The collection and processing of personal data by governments and private corporations raise serious concerns about surveillance, profiling, and misuse of information. Modern technologies enable the continuous monitoring of individuals through smartphones, online platforms, and digital identification systems.[224]

In India, the Supreme Court addressed these concerns in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[225] which recognized right to privacy as a fundamental right under Article 21 of the Constitution. The Court emphasized that informational privacy, including

---

[221] Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2019).
[222] Jack M Balkin, *'The Future of Free Expression in a Digital Age'* (2017) 36 *Pepperdine Law Review* 427.
[223] (2017) 10 SCC 1
[224] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014).
[225] (2017) 10 SCC 1

control over personal data, is an essential component of individual liberty and dignity. The judgment also introduced the proportionality test to evaluate state actions that interfere with privacy.

Freedom of speech and expression is another fundamental right significantly affected by cyberspace governance. Social media platforms and digital communication tools have created new opportunities for citizens to express opinions, mobilize political movements, and participate in democratic debates. However, the digital environment also presents challenges such as misinformation, hate speech, and online harassment.[226]

State Surveillance and Constitutional Safeguards

The expansion of digital technologies has dramatically increased the surveillance capabilities of modern states. Governments can now monitor electronic communications, track online activities, and analyze vast datasets using advanced analytical tools. These surveillance mechanisms are often justified as necessary for combating terrorism, cybercrime, and other threats to national security.[227]

However, ampel surveillance powers increase serious constitutional concerns for the protection of right to privacy and civil liberties. Many surveillance programs may enable governments to accumulate and reserve personal information about citizens without proper safeguards measures. These practices may threaten democracy and collapse the public confidence in state institutions.

Constitutionalism demands that surveillance activities be done within a clearly defined legal framework. State authorities must ensure that surveillance measures are conducted within legal limits, looking for a legitimate objective, and ensure the response is balanced. These requirements make sure that surveillance powers are not used arbitrarily or excessively.

For regulating the surveillance activity, the Judiciary plays an important role. Courts may assess the legality of surveillance laws and analyse whether they are against the constitutional rights. Autonomous bodies and parliamentary committees are there to monitor the implementation of surveillance programs to ensure transparency and accountability.

Another challenge relates to the use of encryption and digital security technologies. Encryption protects the privacy and security of digital communications, but governments often argue that encrypted systems may hinder law enforcement investigations. Balancing the need for strong encryption with the legitimate interests of national security remains a complex issue in cyberspace governance.[228] Ultimately, it should be ensured that effective constitutional safeguards must balance between protecting individual rights and entitle the state to address legitimate security concerns.

---

[226] Jack M Balkin, *'The Future of Free Expression in a Digital Age'* (2017).

[227] Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2019)

[228] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 2006).

Data Protection and Digital Governance

The digital economy relies heavily on the collection and processing of personal data. Governments, corporations, and online platforms gather large volumes of information about individuals' activities, preferences, and communications. While such data can enhance innovation and economic growth, it also creates risks related to privacy, discrimination, and misuse of personal information.[229] Laws on Data protection aim to regulate the collection, storage, and use of personal data. These laws establish rights for individuals and impose obligations on organizations that process personal information. Core principles of data protection typically include consent, transparency, purpose limitation, and accountability.[230]

In India, Digital Personal Data Protection Act, 2023 enacted on August 11, 2023, establishes a framework for processing digital personal data. The law requires free consent for data processing and mandates security mandates by data fiduciaries and imposed penalties for violation of laws. Globally, the most influential data protection regime is the General Data Protection Regulation. It establishes strict rules regarding data processing, including the principles of data minimization, purpose limitation, and accountability. Despite these developments, several challenges remain. One major concern relates to the exemptions granted to government agencies for reasons such as national security or public interest. While such exemptions may sometimes be necessary, they must be carefully regulated to prevent abuse of state power. [231] Another challenge arises from the global nature of digital data flows. Personal data frequently moves across national borders, making it difficult for individual countries to enforce their regulatory frameworks. International cooperation and harmonization of data protection standards therefore play a crucial role in effective digital governance.[232]

Regulation of Digital Platforms and Emerging Constitutional Challenges

Digital platforms have become crucial to contemporary communication and economic activities. Social media networks, search engines, and online marketplaces influence how individuals access information, interact with one another, and participate in public discourse. These platforms often function as modern public forums where democratic debates take place. [233] Governments have increasingly sought to regulate digital platforms to address issues such as misinformation, hate speech, cybercrime, and harmful content. Regulatory frameworks sometimes focus on intermediary liability, which determines the extent to which online platforms are responsible for content posted by users. [234] However, the rules and regulations for digital platforms are raising important constitutional questions. Excessive government dominance on online platforms may lead to censorship or risk of infringing fundamental right to freedom of speech. Conversely, complete hands-off approach can empower the harmful content to spread without accountability. The challenge is in developing regulatory frameworks that balance freedom of expression with the need to maintain a safe and responsible digital environment. Transparency in content moderation policies and accountability mechanisms for

---

[229] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014).
[230] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).
[231] Jack M. Balkin, "*The Future of Free Expression in a Digital Age*" (2017)
[232] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).
[233] Andrew Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2019).
[234] Graham Greenleaf, *Asian Data Privacy* Laws (Oxford University Press 2014)

technology companies are essential for protecting constitutional values.[235] Rapid technological developments also raise new constitutional challenges. Artificial intelligenc, biometric identification etc are increasingly used in public welfare services such as law enforcement, welfare distribution, and financial regulation. While these technologies may improve accuracy and efficiency, they may also create risks related to discrimination, lack of transparency, and degradation of due process. To mitigate these risks, constitutional frameworks must include principles such as algorithmic transparency, accountability, and human oversight. Governments make sure that technological innovation does not weaken the protection of fundamental rights.

Conclusion

The growth of digital technologies and cyberspace governance are facing one of the most significant challenges for contemporary constitutional systems. Governments now having unprecedented capabilities to monitor and regulated digital content personal data and communication, creating a need for new form of "digital Constitutionalism" to protect individual rights from state surveillance and control. While these developments lead to numerous benefits for economic growth and public administration, they also have some serious risks to individual rights and democratic values. Constitutionalism provides the framework necessary to regulate state power in the digital age and ensure that technological governance remains consistent with the rule of law. Protecting fundamental rights in cyberspace requires strong legal safeguards, effective data protection frameworks, transparent surveillance practices, and independent judicial oversight. Courts, legislatures, and regulatory institutions must work together to ensure that digital governance reflects constitutional principles.[236]

As emerging technologies continue to evolve, constitutional systems must adapt to address new challenges such as artificial intelligence, algorithmic decision-making, and cross-border data flows. Ultimately, cyberspace should not exist outside the constitutional order but must be governed by the same principles of legality, accountability, and respect for human rights that define democratic societies[237]

----------**********----------

[235] Jack M. Balkin, "*The Future of Free Expression in a Digital Age*" (2017)
[236] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014).
[237] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (2nd edn, Basic Books 2006).

Chapter 12

Illusion of Absolute Security: From Protection to Surveillance

Koyel Modak, Assistant Professor (Law), Swami Vivekananda University

Abstract

The promise of absolute security has become one of the most powerful narratives shaping contemporary governance, technology, and public imagination. In an age defined by cyber threats, terrorism, data breaches, and geopolitical instability, the demand for complete protection appears both rational and urgent. Yet, the idea of "absolute security" is conceptually flawed and politically consequential. This chapter argues that the pursuit of total protection gradually transforms protective mechanisms into pervasive systems of surveillance, thereby altering the relationship between the state, technology, and the individual.

The illusion lies in the belief that risk can be eliminated. Security, by its nature, is probabilistic. Technological systems are vulnerable, human actors are unpredictable, and threats continually evolve. Nonetheless, political discourse and corporate marketing often portray advanced surveillance technologies as capable of delivering near-total safety. This narrative fosters public consent for intrusive measures by framing privacy as an obstacle to security rather than as its complement.

This chapter critically examines how the shift from protection to surveillance occurs in three interconnected stages. First, it explores the securitization of fear, where exceptional threats are used to justify extraordinary measures. Second, it analyses the technological mediation of security, highlighting how data-driven governance prioritizes predictive control over reactive protection. Third, it interrogates the social consequences of normalized surveillance, including chilling effects on expression, behavioural conformity, and the marginalization of vulnerable groups through algorithmic bias.

Importantly, the chapter does not deny the legitimacy of security concerns. Rather, it challenges the assumption that more surveillance necessarily equates to greater safety. By tracing the historical and theoretical foundations of security discourse, it reveals how the pursuit of absolute protection can undermine democratic values, erode civil liberties, and concentrate power within opaque institutional and corporate structures. The paradox is that measures introduced to preserve freedom may gradually constrain it. The chapter ultimately advocates for a reframing of security as a balanced, accountable, and rights-respecting practice. Instead of striving for unattainable absolutes, policymakers must acknowledge the inevitability of risk and focus on proportionality, transparency, and oversight.

Keywords: *Absolute Security, Surveillance Society, Cyber Security, Data Governance, Digital Privacy, Securitization, State Power, Algorithmic Profiling, Biometric Identification, Risk Management, Civil Liberties, Technological Governance, Mass Data Collection; Predictive Policing; Democratic Accountability.*

Introduction

The contemporary world is increasingly shaped by narratives of security. Governments across the globe justify expansive technological infrastructures and legal frameworks in the name of protecting citizens from threats such as terrorism, cybercrime, and transnational insecurity. While these measures promise enhanced safety, they simultaneously generate complex concerns regarding privacy, civil liberties, and democratic accountability. We would examine the concept of the "illusion of absolute security," arguing that the pursuit of total safety often results in the normalization of pervasive surveillance. This chapter draws an interdisciplinary perspective from law, political theory, and surveillance studies, it explores how security discourses legitimize monitoring practices that extend beyond their original purposes. It further highlights the role of digital technologies, biometric identification systems, algorithmic governance, and public-private partnerships in expanding the scope of surveillance. Despite an extensive body of literature on surveillance and privacy, a critical problem persists in understanding how contemporary societies internalize and normalize surveillance in everyday governance structures while maintaining the belief that such systems guarantee complete protection.[238] This chapter addresses that problem by analysing the structural shift from protective security to surveillance-based governance. It concludes by proposing a rights-based framework that reconciles security objectives with democratic values through transparency, proportionality, and institutional accountability.

Security has historically been a central objective of the modern state. It has long been regarded as the fundamental responsibility of modern state. The legitimacy of political authority has often been justified by the promise of protecting citizens from violence, disorder, and external threats. In the contemporary era, however, the concept of security has expanded beyond traditional notions of military defence and policing. Governments now confront complex threats such as cyber warfare, terrorism, digital espionage, and organized transnational crime. These developments have encouraged the adoption of technologically advanced surveillance systems that monitor individuals, spaces, and communications.

In many contemporary societies, surveillance infrastructures are introduced under the promise of ensuring public safety. Digital monitoring tools, biometric databases, facial recognition systems, and algorithmic risk assessments are presented as necessary instruments to prevent harm. However, the mechanisms used to guarantee such protection as in mass data collection, biometric identification, predictive policing, and algorithmic monitoring have simultaneously expanded state surveillance. Yet these mechanisms also reshape the relationship between citizens and the state. The line between legitimate security practices and intrusive surveillance becomes increasingly blurred.

The notion of absolute security plays a significant role in this transformation. Political narratives frequently suggest that comprehensive monitoring and data analysis can eliminate risks and guarantee safety. However, such promises often obscure the social and legal consequences of surveillance expansion. The pursuit of total security may gradually normalize practices that undermine privacy, autonomy, and democratic oversight. This chapter examines the illusion of absolute security by

---

[238] Julie E Cohen, 'What Privacy Is For' (2013) 126 *Harvard Law Review* 1904.

analysing how protective frameworks evolve into surveillance regimes.[239] It also examines the paradox between the promise of absolute security and the gradual normalization of surveillance practices. It argues that the pursuit of complete security is inherently illusory because it requires intrusive monitoring that can erode civil liberties, privacy, and democratic accountability.[225] It argues that modern security policies rely heavily on technological infrastructures that expand state power while creating new vulnerabilities and rights concerns. The chapter contributes to ongoing debates regarding the balance between security and liberty in the digital age. This chapter explores the illusion of absolute security by examining how contemporary security policies increasingly blur the line between protection and surveillance. It argues that while surveillance technologies can enhance security capabilities, their unchecked expansion risks transforming democratic societies into environments of continuous monitoring. The chapter concludes that democratic societies must critically reassess the narrative of absolute security and instead pursue a balanced approach that safeguards both safety and fundamental rights. Only by acknowledging the limits of security and reinforcing transparency, accountability, and rights-based regulation can societies prevent protection from gradually becoming pervasive surveillance.

Conceptual Foundations: Security, Surveillance and Governance

The relationship between security and governance has long been a subject of political and legal scholarship. Classical theories of the state emphasize that individuals consent to political authority in exchange for protection. According to this perspective, the state functions as a guarantor of security, ensuring order and stability within society.

Modern security governance, however, operates within a far more complex technological and institutional environment. Surveillance technologies have transformed the way states manage risks and monitor populations. Unlike traditional policing methods, digital surveillance allows authorities to collect and analyse vast amounts of information in real time.

Scholars of surveillance studies have observed that modern societies increasingly operate through systems of continuous observation and data collection. These systems are embedded not only within state institutions but also within everyday technologies such as smartphones, online platforms, and digital payment systems. As a result, surveillance has become an ordinary feature of social life rather than an exceptional practice.

The transformation of security governance reflects a broader shift from reactive to preventive strategies. Instead of responding to threats after they occur, modern security systems aim to predict and prevent potential risks. Predictive analytics, behavioural monitoring, and algorithmic profiling are increasingly used to identify patterns that may indicate future criminal or terrorist activity.

The expansion of surveillance is often justified by the argument that modern threats require sophisticated technological responses. Yet this reasoning also raises concerns about proportionality and

---

[239] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Springer 2003) 38. [225] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State* (Metropolitan Books 2014) 95.

accountability. When surveillance becomes pervasive, it alters the relationship between citizens and the state, shifting from trust-based governance to suspicion-based monitoring.

While preventive security offers certain advantages, it also raises important normative questions.[240] The reliance on predictive technologies can result in extensive monitoring of individuals who have not committed any wrongdoing. This shift alters the traditional presumption of innocence and raises concerns about fairness, accountability, and discrimination.

The Expansion of Surveillance Technologies: Rise of Surveillance Society

Technological innovation has dramatically increased the capacity of both governments and private actors to monitor social behaviour. Advances in digital technology have significantly enhanced the capacity of governments and institutions to collect, store, and analyse personal data. Surveillance today is no longer limited to physical observation; it encompasses a vast array of digital processes that operate invisibly within everyday technologies. Contemporary surveillance infrastructures combine multiple forms of data collection, including biometric identification, location tracking, financial records, and digital communications.

Biometric technologies represent one of the most prominent developments in modern surveillance systems. Fingerprint databases, facial recognition tools, and iris-scanning technologies allow authorities to verify identities and track individuals across different contexts. While these technologies are often introduced to improve efficiency and security, they also create centralized repositories of sensitive personal information.

Another significant development is the rise of algorithmic governance. Security agencies increasingly rely on data analytics and artificial intelligence to identify suspicious patterns and predict potential risks. Predictive policing models analyse historical crime data to determine areas that require increased surveillance or policing presence.

The integration of surveillance technologies into everyday infrastructure further complicates the security landscape. Public spaces are now monitored through extensive networks of cameras, sensors, and digital tracking systems. At the same time, private technology companies collect enormous volumes of data through online platforms and digital services.

Moreover, surveillance is not solely conducted by governments. Private technology companies play an increasingly significant role in collecting and managing data. Their platforms generate vast datasets that can be accessed by state authorities through legal mandates or cooperative arrangements. This public-private collabouration further complicates questions of accountability and transparency.

The collabouration between public institutions and private corporations creates new forms of surveillance governance. Governments may access privately collected data for security purposes, while corporations develop technologies that shape surveillance practices. This relationship raises important questions regarding transparency, accountability, and regulatory oversight.

---

[240] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001) 2.

Security Narratives and the Normalization of Surveillance

Public acceptance of surveillance policy measures often depends on the narratives used to justify them and emphasise fear and risk. Governments frequently invoke the language of emergency, threat, and protection to legitimize expanded monitoring powers. In times of crisis, citizens may be more willing to accept intrusive measures if they believe such actions are necessary to ensure safety.

This dynamic can lead to the gradual normalization of surveillance, as described as security narrative, where extraordinary measures become normalized through the language of protection. Temporary measures introduced during periods of crisis may become permanent features of governance. Over time, societies adapt to these practices, and surveillance becomes embedded within routine administrative functions and temporary emergency powers may become permanent features of governance.

The politics of fear can also influence legislative processes. Laws enacted in response to security crises often prioritize rapid action over careful consideration of rights implications. As a result, surveillance authorities may be granted broad powers with limited oversight.

The normalization process is reinforced by the perception that surveillance technologies are neutral and objective. However, these systems are designed and implemented within specific political and institutional contexts. Decisions regarding data collection, algorithmic criteria, and risk assessment often reflect broader social priorities and biases.

While such measures may initially target specific threats, their scope frequently expands. Surveillance technologies introduced for counter-terrorism purposes, for instance, may later be used for routine policing or administrative monitoring.[241]

Moreover, the widespread use of digital technologies encourages individuals to voluntarily share personal information through social media platforms, mobile applications, and online services.[228] This voluntary participation contributes to a culture in which surveillance becomes both institutional and self-imposed.

Data, Algorithms, and Predictive Security

One of the most significant developments in modern surveillance is the integration of algorithmic analysis into security systems. Predictive policing tools analyse historical crime data and behavioural patterns to anticipate potential incidents. Similarly, border security systems use risk-assessment algorithms to identify individuals considered suspicious.

Although these technologies promise greater efficiency, they also raise serious ethical and legal concerns. Algorithms rely on datasets that may reflect existing social biases. When such data are used to predict risk, they can reinforce discriminatory patterns in policing and law enforcement.

---

[241] Daniel J Solove, *Nothing to Hide: The False Trade-Off Between Privacy and Security* (Yale University Press 2011) 3.
[228] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015) 67.

Furthermore, algorithmic decision-making often lacks transparency. The criteria used to determine risk scores or threat assessments may not be publicly accessible. This opacity makes it difficult for individuals to challenge decisions that affect their rights.

Another concern relates to data centralization. Large-scale security databases combine information from multiple sources, including biometric records, financial transactions, travel histories, and online communications. The concentration of such sensitive data increases the risk of misuse, unauthorized access, or data breaches.

Specifically, there is limited research addressing how security narratives construct the perception that surveillance technologies can guarantee complete safety, thereby legitimizing the expansion of monitoring infrastructures. This chapter addresses that gap by examining the relationship between security discourse, technological governance, and the social acceptance of surveillance.

By analysing the illusion of absolute security, the chapter highlights how political narratives shape public perceptions of risk and protection. It also demonstrates that surveillance expansion is not solely driven by technological capability but also by the cultural and institutional belief that more monitoring inevitably leads to greater safety.

Legal and Human Rights Implications

The expansion of surveillance raises significant legal and ethical concerns. Privacy is widely recognized as a fundamental human right, essential for protecting individual autonomy, dignity, and freedom of expression. [242] Excessive monitoring can undermine these rights by creating an environment in which individuals feel constantly observed.

Legal frameworks attempt to balance security interests with individual rights through principles such as necessity, proportionality, and legality. Surveillance measures should therefore be justified by legitimate objectives and implemented only to the extent required to achieve those objectives.

However, contemporary surveillance infrastructures often operate on a scale that challenges traditional legal safeguards. Mass data collection and algorithmic decision-making can occur without meaningful public oversight or transparency. A key challenge lies in ensuring that surveillance measures remain proportionate and necessary. Broad or indiscriminate data collection may conflict with constitutional principles and human rights standards. Courts in various jurisdictions have increasingly scrutinized surveillance laws to determine whether they adequately protect individual liberties.

Another important concern relates to data security. Centralized databases containing biometric or behavioural information present significant risks if they are misused, hacked, or accessed without authorization. Data breaches involving sensitive personal information can have long-term consequences for individuals and institutions alike. Another significant issue concerns the role of private corporations in surveillance infrastructures.[230] Technology companies that manage communication networks, cloud storage, and digital platforms possess vast quantities of user data.

---

[242] *Universal Declaration of Human Rights* (adopted 10 December 1948 UNGA Res 217 A(III)) art 12.
[230] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 8.

When governments seek access to such data, questions arise regarding jurisdiction, consent, and the limits of corporate cooperation with state authorities.

Courts in various jurisdictions have increasingly recognized the importance of privacy protections in the digital age. Judicial decisions have emphasized that technological advancements must not erode the fundamental rights that underpin democratic societies.

The Illusion of Absolute Security

The pursuit of absolute security is inherently problematic because complete protection from all threats is unattainable. Societies are inherently dynamic and complex, and new forms of risk continuously emerge. Attempting to eliminate every potential threat would require an unrealistic level of control over social behaviour.

The belief in absolute security therefore functions as a political and technological myth. Surveillance systems can reduce certain risks, but they cannot eliminate uncertainty entirely.[243] In fact, excessive reliance on surveillance may generate new vulnerabilities, including data misuse, institutional overreach, and technological dependence.

Furthermore, large-scale data collection can create information overload for security agencies. When authorities must analyse enormous datasets, identifying genuine threats becomes more difficult rather than easier. The pursuit of total security may therefore reduce rather than enhance effectiveness.

Recognizing the limits of security is essential for maintaining democratic values. Instead of striving for unattainable certainty, societies must focus on building resilient institutions that can respond effectively to emerging threats while respecting fundamental rights.

The illusion of absolute security therefore lies in the belief that technological surveillance can fully eliminate uncertainty. In reality, security strategies must acknowledge the limits of prediction and control.

Towards Balanced Security Governance and Rights-Based Security Framework

A balanced approach to security governance requires rethinking the relationship between protection and surveillance. Several policy recommendations can help address the challenges identified in this chapter.

1. Strengthening Legal Safeguards

Surveillance practices must operate within clear legal frameworks that define the scope and limitations of monitoring powers. Laws should specify the purposes for which data may be collected and ensure that surveillance activities are subject to judicial authorization.

---

[243] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, Vintage Books 1995) 195.

2. Enhancing Institutional Oversight

Independent oversight bodies should be empowered to review surveillance practices and investigate potential abuses. Parliamentary committees, data protection authorities, and judicial institutions can play crucial roles in ensuring accountability.

3. Promoting Transparency

Transparency is essential for maintaining public trust. Governments should provide clear information regarding the technologies used for surveillance, the types of data collected, and the safeguards implemented to protect individual rights.

4. Implementing Privacy-by-Design

Technological systems should incorporate privacy protections at the design stage. Data minimization, encryption, and decentralized storage can reduce the risks associated with large-scale data collection.

Conclusion

The relationship between security and surveillance represents one of the defining challenges of the digital age. The pursuit of absolute security represents one of the most significant paradoxes of modern governance. While surveillance technologies promise protection against emerging threats, they also risk undermining the fundamental freedoms that democratic societies seek to protect.[244]

This chapter has argued that the belief in total security is largely illusory. Surveillance systems cannot eliminate uncertainty, and their unchecked expansion may create new vulnerabilities and rights concerns. By identifying a critical research gap in understanding how security narratives normalize surveillance, the chapter contributes to broader debates within legal and political scholarship. Ultimately, the challenge for contemporary societies lies in maintaining a delicate balance between safety and liberty. A sustainable approach to security requires recognizing that safety and liberty are not mutually exclusive but must be carefully balanced. Security policies must be grounded in principles of transparency, accountability, and respect for fundamental rights. Only by acknowledging the limits of surveillance and strengthening democratic safeguards can societies prevent the transformation of protective governance into pervasive monitoring. By reinforcing transparency, accountability, and rights-based regulation, societies can ensure that the pursuit of protection does not gradually transform into a regime of pervasive surveillance.

_______________*****************_______________

[244] David Lyon, *Surveillance Studies: An Overview* (Polity Press 2007) 14.

Chapter 13
Beyond Firewalls: Copyright, AI Content, and the Cybersecurity Reality Check

Abu Zar, Assistant Professor, School of Legal Studies, Swami Vivekananda University

Abstract

Cybersecurity has historically been viewed as being a technical-based discipline such as firewalls, encryption and intrusion-detection systems[245]. With the rapid adoption and spread of artificial intelligence (AI) in the creation of content, we have now entered a new phase of Digital Security, which combines copyright law with Intellectual Property Rights (IPR) at the intersection of AI-generated content with cyber security[246]. This chapter will show how the commonly-held view that cyber security is a solely technical discipline has blinded us to the fact that legal loopholes — many of which stem from AI-generated content — can represent significant threats to cybersecurity as well.

The introduction of generative AI has introduced disruptions to existing copyright systems, which have traditionally been structured around human authorship[247]. As a result, many questions remain about originality, ownership and liability for works created by AI, meaning that they exist in a legal grey area. Courts and legislators across the globe have struggled to apply established concepts of copyright law in the context of machine-generated creations, such as whether works generated by machines can be protected under copyright law and whether existing copyright holders have been infringed by the use of their protected materials to train the AI systems that produce these works[248]. These issues have major relevance to the cyber security space since malicious actors are using ambiguities in copyright as a means of perpetrating takedown abuse, spreading of misinformation and perpetrating data poisoning attacks through the weaponization of intellectual property disputes in cyberspace.

This chapter situates the issues discussed herein against the greater Cybersecurity Myth-Reality Divide. It will examine where copyright disputes interact with threats emanating from the cyber domain, showing how the lack of a clear legal framework erodes confidence in the digital ecosystem. It does so by relying on several increasingly prominent scholarly articles related to these matters, such as Jiang et al.'s Blockchain Enabled Approaches to AI Copyright Management[249]; Yang & Zhang's Economic Modelling of Fair Use and AI Copyrightability[250]; and Muthu's analysis of current Indian and International Copyright Law[251]. As such, all sides will have access to both the global and jurisdictionally specific aspects of the challenge at hand.

---

[245] Christopher T Zirpoli, *Generative Artificial Intelligence and Copyright Law* (CRS, 2025).
[246] Astha Ojha, *AI & Copyright in India: Law, Policy, and the Future of Creative Rights* (MeitY, 2024).
[247] Asmi Vikas Kedare, 'The Impact of Generative AI on Copyright Law in India' (SSRN, 2024).
[248] ibid.
[249] Jiang et al, 'Blockchain Enabled Approaches to AI Copyright Management' (2023) JIPTL 45.
[250] Yang & Zhang, 'Economic Modelling of Fair Use and AI Copyrightability' (2022) IRLE 71.
[251] Muthu, 'Analysis of Current Indian and International Copyright Law in the Age of AI' (2023) IJLT 19(2).

The chapter will also argue that to achieve strong cybersecurity, it will be necessary to build upon both technical defences as well as strong legal and/or policy frameworks to meet the real-life challenges submitted by AI to traditional perceptions regarding copyright ownership.

Ultimately, the chapter will call for hybrid solutions that bring together law, technology and policy. By bridging the gap between the legitimate and illegitimate perceptions of ownership and the actualities created by AI-based content creation, the chapter aims to develop a blueprint for how to secure digital creativity in a world dominated by generative AI[252]. The chapter will also assist in furthering the overall realm of Beyond Firewalls which highlights how to build a successful cybersecurity infrastructure through the recognition and mitigation of the inherent legal risks associated with digital innovation.

Keywords: *International Copyright Law, Firewalls, Encryption And Intrusion-Detection Systems.*

Introduction: Cybersecurity Beyond the Technical Lens

Traditionally, cybersecurity is seen as a strictly technical field comprised of firewalls, encryption methods, and intrusion detection systems[253]. Nevertheless, that viewpoint only tells a piece of the story; in reality, cybersecurity has many legal, social, and ethical issues associated with it – especially now that we are living in an era where AI is changing what we understand as creative works[254]. As automated creativity continues to produce new forms of text, images, music, and code, the scope of traditional intellectual property law will be pushed to its limits. Therefore, it is a myth that cybersecurity can be achieved through technical means alone because, at the same time, new questions regarding the authorship, ownership, and liability of AI-generated content create additional vulnerabilities and risk of exploitation[255].

Thus, many aspects of copyright law which were developed with the evaluation of human creativity have now been disrupted by the increasing prevalence of generative AI. Historically, copyright law has assumed that a human author creates a work using their skills, judgement, and originality to produce an expression that is eligible for copyright protection. Conversely, it is now possible for an AI system trained on millions of sets of data to generate outcomes that are like human creativity though there was not an actual human author involved in producing the outputs in question. Consequently, two important issues arise: (1) whether AI-generated works are eligible for copyright protection; and (2) who should receive credit as the author of an AI-generated work? Answering these questions are important from the perspective of cybersecurity because unresolved issues of ownership provide significant opportunities to exploit others[256].

---

[252] Zirpoli (n 2).
[253] Zirpoli (n 2).
[254] Ojha (n 3).
[255] Kedare (n 4).
[256] ibid.

Adversaries can exploit copyright-based claims to impede operations across digital platforms by filing false claims or issuing bogus takedown notices, thus allowing them to disrupt digital platforms, disseminate misinformation, or damage confidence levels among the members of online systems at scale[257]. Because of these dynamics, the difference between the myth and reality is much more pronounced than typical cases of disagreement between claims of property rights and the real rights attached to an object.

The myth is that generative (AI produced) media is completely "free" or "ownerless," thus creating an argument that it can be used by anyone without restrictions. In contrast, the reality is that while generative content may exist, it exists in an area where the ability to determine who is liable or entitled to use generative content is constantly shifting due to competing claims of ownership or use of that material[258]. As generative technologies create new types of vulnerabilities and introduce new issues related to cybersecurity, it is necessary to protect and privilege existing intellectual property laws as part of the underlying protection of any content available to the public.

A growing body of literature has begun creating avenues for addressing these issues through the application of existing, recent works. Jiang et al. offer blockchain based frameworks for managing generative media leveraging concepts related to maintaining trust-based lifecycle records and executing trusted, independent third-party audits throughout the entire life of the media[259].

In their article, Yang and Zhang look at how both copyright law and fair use impact the economics of generative AI[260]. They discuss the ongoing conflict between promoting innovation and regulating it. Muthu analyses both Indian and international copyrights and examines how each jurisdiction has a different set of challenges to incorporating AI into their respective statutory frameworks[261]. The combination of these two studies demonstrates that the notion that AI-generated creativity is clear and defined ownership has failed; AI creativity exists in a fragmented and contentious environment and is inherently tied to cybersecurity issues.

This chapter examines this debate in relation to the wider context of the 'myth-reality divide' in cybersecurity. The chapter develops the argument that that effective cybersecurity requires not only technical defences but also legal and policy structures that can adapt to deal with the realities of AI-generated creativity[262]. It uses a framework examining the relationship between copyright law, AI content, and cybersecurity to illuminate the myths that prevent the understanding of these vulnerabilities and to highlight the realities that must be addressed. Therefore, it supports a broader understanding of cybersecurity as a whole—an understanding that incorporates both technical and legal factors to provide security to digital creativity.

---

[257] Zirpoli (n 2).
[258] Muthu (n 8).
[259] Jiang et al (n 6).
[260] Yang & Zhang (n 7).
[261] Muthu (n 8).
[262] Ojha (n 3).

The Myth of AI Creativity and Ownership

There are many myths surrounding artificial intelligence and one of them is that AI-generated works are neutral (i.e., unbiased), free (i.e., chargeable to no person), and unowned (i.e., unowned by anyone)[263]. Part of this myth stems from a belief that machines cannot create nor claim authorship as they don't possess the same capacity to create because they're machines. However, the truth is much more complicated. Generative AI is trained on huge amounts of data and produces works with some quality of originality and artistic merit. Thus these "neutral" speaking outputs exist in a contested legal and moral environment[264].

Copyright has been historically defined based on human authorship. Under the Berne Convention, copyright assumes creative works will come from identifiable people who can exert intellectual effort into creating the output[265]. Additionally, The TRIPS Agreement also places copyright within trade and enforceable structures and promotes a human-centred approach[266]. Therefore, generative AI disrupts this basis of all established rules of copyright law as they produce works without any direct involvement by humans. Thus, courts and lawmakers have had difficulty deciding whether to protect generative AI works under existing copyright law. For example, the US Copyright Office has explicitly ruled that works solely created by a generative AI are not entitled to copyright protection[267], thus further entrenching the belief that the output of a generative AI has no legal significance.

The "Myth of the Free Content" is another example of how AI's creative capacities are ignored, including the economic and ethical implications associated with the use of creativity created by Artificial Intelligence (AI)[268]. AI's reliance on datasets to develop and produce creative work often has significant implications for copyright law and the concept of fair use, as training data sets frequently include works subject to copyright protection. Because many AI-based systems use creative work protected by copyright law to generate their output, the resulting creative work should not be regarded as neutral and free from any legal obligations. As a result, both users and developers of AI-generated creative works risk being held liable, which undermines the perception that AI creativity exists outside of the sphere of protection offered under Intellectual Property law[269].

Scholars have expressed concern that allowing this myth to persist creates risk for the future of creative industries. For example, Andres Guadamuz posits that by removing AI-generated works from copyright protection, the creative economy would be negatively impacted because unlimited exploitation of original creative works would occur without compensating the original creator[270]. Similarly, Pamela Samuelson stresses that copyright law must adapt to the digital world in which we live, including the unique way Artificial Intelligence produces creative works, to preserve copyright's

---

[263] Zirpoli (n 2).
[264] Kedare (n 4).
[265] Berne Convention for the Protection of Literary and Artistic Works (Paris Act 1971).
[266] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, 1994).
[267] US Copyright Office, *Copyright Registration Guidance: Works Containing AI-Generated Material* (2023).
[268] Samuelson (n 28).
[269] Yang & Zhang (n 7).
[270] Andres Guadamuz, 'Artificial Intelligence and Copyright' (2017) WIPO Magazine.

legitimacy[271]. Yang and Zhang provide an economic analysis of the relationship between Copyright and Fair Use by providing a mathematical model demonstrating how allowing unlimited use of generative AI-created works would eliminate incentives to innovate in the creative community[272]. Finally, Muthu's analysis of the law in India emphasises that the lack of clear, enforceable rules in relation to AI-generated creative works creates uncertainty in cyberspace, which can result in the exploitation of those works by individuals and/or entities that reside outside of the jurisdiction of the creator[273].

Thus, it follows that AI Creative must be viewed in the larger picture of the ecosystem around it which includes the rights, obligations and exposure of this ecosystem to security risk[274]. As ownership, liability and ethical issues are inseparable from the risk of Generative AI technology publicly exposing the myth of neutrality while exposing the reality of contestable nature of AI Creative, this chapter highlights the fact that the complexities of machine-generated content must be recognised and reflected in legal constructs.

Copyright in the Age of Generative Algorithms

The rise of generative algorithms has had significant effects on copyright law[275]. Copyright laws were originally created for human creators and are based on the idea that creative works are the outcome of the expertise of an individual. When it comes to generative AI, though, the output is created without much involvement from the artist or human creator. Because there is no human author creating an art piece, it is not clear whether it meets the requirements of copyright law with respect to originality and authorship[276].

International treaties such as the Berne Convention and TRIPS Agreement do not address this issue, meaning that they support copyright based on human authors[277]. In practice, different countries have responded differently to this problem; for example, the US Copyright Office has decided that they will not protect works that were created by AI alone[278], while the UK Intellectual Property Office has allowed for limited recognition of works created with assistance from AI[279].

Copyright has become highly debated when it comes to AI-created works, especially with respect to originality. Courts have required "a minimal amount of creativity" or "a substantial degree of intellectual effort" for the establishment of copyright[280], and the originality of an AI-produced work is less certain than a traditional creative work because AI-generated works lack human intention. Guadamuz and others have pointed out that excluding AI works entirely might undermine the creative

---

[271] Pamela Samuelson, 'Copyright Law and the Digital Age' (2019) *Journal of Intellectual Property Law*.
[272] Yang & Zhang (n 7).
[273] Muthu (n 8).
[274] Muthu (n 8).
[275] Zirpoli (n 2).
[276] Kedare (n 4).
[277] Berne Convention (n 22), TRIPS Agreement (n 23).
[278] US Copyright Office (n 24).
[279] UK Intellectual Property Office, *Consultation on Artificial Intelligence and Copyright* (2021).
[280] US Supreme Court, *Feist Publications v Rural Telephone Service Co* 499 US 340 (1991).

industry[281], while authors such as Weatherall caution that including AI works might dilute the concept of authorship[282].

With respect to liability, there is great uncertainty about who would be liable if an AI-created work is infringing: the developer of the AI, the user or any of the prior datasets[283]. This uncertainty has ramifications for cybersecurity—as malicious actors can exploit the lack of clarity in liability rules to publish infringing or harmful materials and give little (or no) attribution/accountability to any party.

Recent approaches have suggested hybrid solutions. Giblin and Weatherall have stressed the importance of ensuring that any dataset used to train an AI meets copyright obligations through using a transparent dataset[284]. Jiang et al are proposing blockchain-based systems to provide for accountability and tracing back through the lifecycle, allowing an AI-generated work to be traced back to its source(s)[285]. These types of approaches support the conclusion that to adequately protect AI-generated works, legal protections need to be in place which incorporate technological safeguards.

In summary, copyright for AI-generated works is currently fragmented and contested, but large developments are likely to occur soon[286]. The perception that ownership can be clearly defined has been replaced by an understanding that there is a considerable amount of uncertainty over various aspects of cyberspace. Laws and treaties at both the nation-state and international level, as well as substantial academic discourse surrounding the subject, have not kept up with the rapidly evolving landscape of technology. Beyond being a legal issue, uncertainty creates risks associated with the security of digital ecosystems, resulting in a loss of confidence in cyberspace and exposing opportunity for exploitation[287].

Intersecting Domains: Copyright Disputes as Cybersecurity Risks

Digital vulnerabilities resulting from the intersection between copyright law and cybersecurity are one of the most critical yet underappreciated areas of research[288]. Historically, copyright issues revolved around ownership and infringement, but copyright is now used as a source of cyber conflict with both malicious uses of copyright law and intellectual property as a means of disrupting digital platforms through the weaponization of takedown notices, automatic content filter systems, and threats of lawsuits[289].

One illustration of how copyright is exploited as a source of cyber disruption is through the misuse of the Digital Millennium Copyright Act (DMCA) takedown provision[290]. The DMCA was designed to

---

[281] Andres Guadamuz, 'Artificial Intelligence and Copyright' (2017) WIPO Magazine.
[282] Kimberlee Weatherall, 'AI and the Concept of Authorship' (2020) *UNSW Law Journal*.
[283] Samuelson (n 28).
[284] Rebecca Giblin and Kimberlee Weatherall, 'AI Training Data and Copyright Transparency' (2022) *Journal of Intellectual Property Law & Practice*.
[285] Jiang et al (n 6).
[286] Muthu (n 8).
[287] Yang & Zhang (n 7).
[288]Zirpoli (n 2).
[289] Kedare (n 4).
[290] Digital Millennium Copyright Act 1998 (US).

protect the rights of copyright owners but has been misused to silence competitors, promote misinformation, or otherwise disable legitimate content. Viewed through the cybersecurity lens, this represents a legal denial of service attack against online systems and thus erodes confidence in the online economy.

The proliferation of generative AI technologies complicates this issue. For example, deepfakes and synthetic media created by training on copyrighted materials result in a grey area that blurs between legal infringement and manipulation[291]. Where copyright disputes involve disinformation campaigns, the confluence of copyright and cyber threats creates a hybrid threat with both legal uncertainty and technical exploitation. This convergence of copyright and cybersecurity shows that copyright is no longer at the periphery of cybersecurity but is crucial to its integrity.

The response to policies is inconsistent and lacking. While the EU Digital Services Act sets an obligation on platforms to tackle illegal activity online, i.e., copyright issues, etc., it does not have fully developed methods for enforcing it yet[292]. In addition, as Bruce Schneier points out, there are equally as many risks when it comes to the law itself containing legal vulnerabilities as there are with technology - adversaries will exploit whichever vulnerability offers them the greatest access[293].

Copyright disputes now operate as vectors for creating cyber insecurity; therefore, if policymakers and scholars can identify this intersection, they could take steps to end the myth that intellectual property laws are in some way different than those governing cyber security[294]. Owners of intellectual property rights and the material they own are continuously in conflict; there are gaps in liability coverage; and enforcement mechanisms are needed to provide the stability needed in digital networks.

Case Studies: Law, AI, and Digital Vulnerabilities

Copyright disputes intersect with cybersecurity risks in practice, and case studies provide concrete examples of the way these two areas intersect. Generative AI presents challenges that are not just theoretical--but rather are posed by real legal conflicts and risks posed by technologies used to create generative AI[295].

A notable example is the case concerning AI-generated art platforms. A group of artists filed suit against Stability AI based on allegations of infringement of their works by Stability AI's training datasets (2023)[296]. This case illustrates how unresolved questions concerning the legality of the datasets used for training generative AI can lead to a large-scale dispute and cybersecurity risks. If the training data is unlawfully obtained or manipulated, the resulting generative AI images can create both legal

[291] Samuelson (n 28).
[292] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).
[293] Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (WW Norton 2018).
[294] Muthu (n 8).
[295] Zirpoli (n 2).
[296] *Andersen et al v Stability AI Inc* (US District Court, ND Cal, filed 2023).

liability and reputation damage for the platform(s) that use the training data to create generative AI images.

Another example of legal jeopardy related to generative AI and cybersecurity is the use of deepfake technology in political campaigning. Courts and regulators regularly wrestle with legal issues concerning whether deepfakes are a form of copyright infringement, defamation, or a threat to the cybersecurity of political campaigns[297]. The difficulty with applying established legal categories to AI outputs is illustrated by the hybrid nature of deepfakes (creative, deceptive, or potentially infringing), which makes it difficult for courts to determine the applicability of traditional legal categories.

Additionally, in India, the issue of copyright in respect of AI-generated educational material has raised jurisdiction-specific issues related to cybersecurity[298]. Institutions lack necessary statutory guidance to make determinations as to whether AI-generated materials may be owned, licensed, or protected. Because there is no certainty about how to handle copyright violations across different jurisdictions (countries) and continents (areas), this creates the possibility that bad people will capitalize on the gap left by enforcement (those "bad actors") and destroy trust in digital learning systems (the Internet).

The case study presented in this chapter support a larger theme within this chapter: that copyright issues are not just an isolated legal problem, but also a cybersecurity issue[299]. They also show how ownership issues, lack of liability, and lack of an effective (or even appropriate) means of enforcing copyright protection can lead to a breakdown in the digital world and illustrate that technical cybersecurity by itself does not exist.

Global Legal and Policy Perspectives

Artificial intelligence governance and the intersections of copyright and data security law are widely disparate[300]. Instead of a coherent international standard, we see a collection of divergent nations' laws, regional regulations, consultation forums, and other policies. The diverse landscape is more than a technical challenge—it is a dereliction of the fundamental infrastructures. Because rules differ across borders, nations, regions, and continents create avenues for individuals to use technological loopholes to exploit weaknesses in copyright enforcement and undermine the resilience of organizations to respond to cybersecurity vulnerabilities[301].

European Union: A Holistic Approach

AI regulation in Europe is leading the world. The AI Act creates a risk-based classification system for AI systems that sets strict requirements for transparency, accountability, and documentation of datasets from high-risk AI system providers[302]. Although the AI Act is not a copyright law, it indirectly

---

[297] Chesney and Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.
[298] Muthu (n 8).
[299] Kedare (n 4).
[300] Zirpoli (n 2).
[301] Kedare (n 4).
[302] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final.

influences the debates about who owns the copyright by establishing a requirement for provenance records for training data. This means that the use of datasets that include protected works is problematic in the copyright context for most generative models. The European Union expects that by creating a mandatory disclosure requirement, it can reduce infringement risk and increase cybersecurity through traceability.

The **Digital Services Act (DSA)** helps create an EU-wide regulatory framework by requiring platforms to remove all illegal content from their services, including content that infringes on copyrights, within a specified time frame[303]. The AI Act and DSA work collabouratively as part of an overall regulatory approach where copyright enforcement is a component of the larger digital governance process and is inextricably linked to cybersecurity. The EU is positioned as a normative leader in this area and seeks to export its regulatory regime globally through trade agreements and digital partnerships[304].

United States: Fragmentation and Litigation

In comparison to how it has responded, the United States government is fragmented and typically responds reactively. The Copyright Office has issued clarifying opinions that deny copyright to anything made by only an artificial intelligence, thereby upholding a fundamentally human-based model of authorship. But there are no federal statutes yet regulating the use (and/or creation) of artificial intelligence[305]. Rather, private parties are responsible for mostly enforcing the current copyright laws through traditional litigation as well as by acting under the **Digital Millennium Copyright Act ("DMCA")[306].** Additionally, the current DMCA system has been used by malicious actors to attack others. Copyright claims are often used strategically by competitors (i.e., the person asserting copyright over a protected work and/or the company asserting copyright over the work) to disrupt the ability of legitimate parties to provide their product/content to the market or to disrupt their ability to use a particular platform — in essence, to create a denial of service through lawful processes[307].

This reliance on a litigation-based system creates uncertainty about cybersecurity (which has also increased in recent years). In this sense, the copyright system and the cybersecurity system remain separate; however, they are becoming increasingly dependent on one another. The US approach is consistent with a market-driven philosophy of governance, but it is riddled with many substantial gaps that adversarial parties can take advantage of.

---

[302] Digital Services Act (n 49).
[303] ibid
[304] US Copyright Office (n 24).
[305] DMCA (n 47).
[306] Samuelson (n 28).
[307] Guadamuz (n 27).

Asia: Hybrid Models and Cautious Approaches

There are varied approaches taken by Asian countries about this area. For example, China has issued regulations governing deep synthesis technologies, which require those who operate or create synthetic content to identify themselves, as well as preventing the misuse of synthetic content[308]. These obligations link the enforcement of copyright with cybersecurity and recognize that the production and distribution of synthetic media have both legal implications and security risks. By having these requirements in place, China hopes to limit disinformation campaigns and protect the rights of content creators.

India has not legislated on the issue of creativity produced through AI technologies to date; however, Indian courts and scholars have made it clear that human authorship is the fundamental basis for copyright protection and have taken a conservative approach to extending the protection of copyright to works created by machines[309]. This conservative approach avoids giving legal recognition to the authorship of AI-generated works currently, but results in limited enforcement mechanisms against those who engage in producing and distributing such works. Practically speaking, this uncertainty creates significant exposure to risks for organizations, platforms, and other stakeholders who are susceptible to being exploited by individuals using malicious tactics that benefit from existing regulatory uncertainty.

International Organisations: The Struggle for Harmonisation

The World Intellectual Property Organization (WIPO) has started an initiative on the relationship between artificial intelligence and intellectual property law on an international level, with the goal of garnering input on this topic[310]. The urgency of harmonizing international intellectual property laws has become apparent because of the international nature of disputes regarding the creation of works by artificial intelligence. However, few countries have come to agreement about how laws will be harmonized, and developed countries tend to advocate for the incentive to develop innovation; developing countries are more apt to support equitable access and protection from the exploitation of creative works[311].

The lack of agreement on how the use of artificial intelligence should be regulated has led to the escalation of copyright disputes regarding works created by artificial intelligence being thrown into questions of jurisdiction[312]. An example of this would be when local law adheres to the local exception for copyright protection and the creation of the work is illegal outside of that country. The lack of international cognition regarding copyright dispute resolution leads to a set of issues related to trust in the digital ecosystem as well as systemic vulnerabilities.

---

[308] Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (2022).
[309] Muthu (n 8).
[310] World Intellectual Property Organization (WIPO), *WIPO Conversation on Intellectual Property and Artificial Intelligence* (2020).
[311] ibid.
[312] Yang & Zhang (n 7).

Towards Convergence

There is evidence that there are some trends moving parties toward a convergence of opinions and laws regarding artificial intelligence, including an increasing emphasis on transparency in relation to the training dataset, accountability for outputs and liability of parties for the misuse of training datasets and/or the outputs created from them[313]. These principles suggest an acceptance that there are interdependencies between copyright and the cybersecurity community relative to their respective roles in developing a governance system for digital commerce. Moving forward, the challenge will be to create enforceable international covenants between all parties regarding these principles[314].

Bridging the Divide: Towards Hybrid Legal–Technical Solutions

Due to the ongoing global fragmentation of copyright laws and the rapid advancement of generative artificial intelligence (AI) technologies, there is an urgent need for hybrid solutions that bring together legal and technological measures[315]. While both laws and technologies can assist in addressing the challenges posed by AI generated materials individually, it is the shared responsibility of each discipline to effectively address these challenges. Addressing the legal challenges presented by AI consists of providing a comprehensive strategy that incorporates norm-based regulation along with technical measures. There are copyright litigation challenges; liability gaps for products used by AI; and cybersecurity risks associated with AI that require coordinated solutions combining traditional regulatory mechanisms with innovative technological solutions.

The Limits of Purely Legal Responses

Generative algorithms are too complex for traditional copyright law[316]. The requirement for human authorship remains theoretically sound, the real-world problem lies in the non-human nature of autonomous creativity via machines. The judicial and legislative branches of government have had difficulty identifying how to respond too many courts and legislatures have resorted to narrowly interpreting traditional copyright laws thus denying copyright protection for certain passive forms of AI outputs. This provides protection of the integrity of an authorship; however, passive forms of AI outputs circulate within the marketplace without clear affiliation to any party which creates ambiguity amongst creators, platforms and users.

In addition, enforcement methods that are based solely on legal remedies have been shown to be ineffective, particularly in a cyberspace context, where they tend to fall within the reactive category of remedy, rather than the proactive category of remedy. As a result, once a court or other legal body has concluded that there is an infringement, it does not cure the harm or resolve the underlying issues because of the inherent delay in investigations and resolution processes[317] unique to cyberspace, and

[313] Giblin and Weatherall (n 41).
[314] ibid.
[315] Zirpoli (n 2).
[316] US Copyright Office (n 24).
[317] Samuelson (n 28).

as a result, malicious actors exploit this ambiguity to disseminate infringing or harmful content without consequence.

Generative algorithms are too complex for traditional copyright law. The requirement for human authorship remains theoretically sound, the real-world problem lies in the non-human nature of autonomous creativity via machines. The judicial and legislative branches of government have had difficulty identifying how to respond too many courts and legislatures have resorted to narrowly interpreting traditional copyright laws thus denying copyright protection for certain passive forms of AI outputs. This provides protection of the integrity of an authorship; however, passive forms of AI outputs circulate within the marketplace without clear affiliation to any party which creates ambiguity amongst creators, platforms and users.

In addition, enforcement methods that are based solely on legal remedies have been shown to be ineffective, particularly in a cyberspace context, where they tend to fall within the reactive category of remedy, rather than the proactive category of remedy. As a result, once a court or other legal body has concluded that there is an infringement, it does not cure the harm or resolve the underlying issues because of the inherent delay in investigations and resolution processes unique to cyberspace, and as a result, malicious actors exploit this ambiguity to disseminate infringing or harmful content without consequence.

The Limits of Purely Technical Responses

Technical safeguards like watermarking, dataset transparency and blockchain based provenance offer new possibilities for managing AI output. Jiang et al suggest using blockchain technology to create a lifecycle record that will allow for traceability[318] of AI generated works. Watermark technologies can embed identifying information within synthetic media, allowing for the identification and prevention of misuse of those media.

However, technical solutions alone cannot answer normative questions regarding ownership, liability, and authorship[319]. While watermarks may provide evidence of provenance, they do not determine copyright status. Although blockchains will provide a record of the lifecycle of a work, they cannot resolve disputes regarding fair use or infringement. Without legal recognition, these technical safeguards may go unused or be ignored.

Towards Hybrid Governance

Hybrid governance models look to merge the legal and technological ways to govern through copyright and cybersecurity, given the interconnectedness of the two areas, and necessitating a collabourative approach to ensuring adequate regulation on both fronts.

An approach of how this is occurring is through embedding legal duties into technical architecture[320], such as when the EU's AI Act imposes requirements for transparency regarding training datasets; this

[318] Giblin and Weatherall (n 41).
[319] EU AI Act (n 49);
[320] Digital Services Act (n 49).

legal obligation can be fulfilled using technical solutions like dataset registries or blockchain records. As a result of the integration of both legal and technical solutions, compliance with these legal duties would not only be a matter of being declared but also providing verifiable technology for compliance.

Another approach of how interconnectedness between copyright and cybersecurity will provide an improved governance model is through establishing liability frameworks that allocate responsibility across all stakeholders; developers, platforms, and users should share some amount of responsibility for the output of AI technologies and use technical safeguards as evidence of legal accountability. For instance, if a platform incorporates watermarking to identify synthetic media that is deployed on a platform, but the platform does not act when that synthetic media is identified, the platform may be liable based on its failure to meet its obligation to act against illegal activity. By providing an incentive for legal compliance as well as for due diligence with respect to compliance, the hybrid approach will advance governance models for both copyright and cybersecurity.

Ethical and Policy Dimensions

There are ethical considerations that must be addressed in hybrid solutions. There is a moral obligation as well as a legal one to make datasets transparent to honour the rights of the creator in the dataset. There are also technical issues associated with watermarking technologies. These watermarking technologies must balance privacy with detection. Watermark technologies must have the capability to detect a watermark without being able to reveal any confidential information about an individual. Policymakers will need to develop frameworks that provide for ethical safeguards in both law and technology. They will need to develop these frameworks with the understanding that legitimacy cannot be achieved solely through compliance. International cooperation is necessary for hybrid solutions to be successful. WIPO's consultations on AI and IP clearly demonstrate the need for cooperation and harmonization[321] about AI and IP. However, an agreement on how to accomplish this has yet to be reached. Hybrid solutions may be the best way to reach a compromise. Hybrid solutions will allow states to adopt flexible technical standards while still meeting the requirements established by core principles of law. For example, states could agree to minimum requirements regarding the transparency of datasets but could allow for the local enforcement of those minimums.

Case Studies in Hybrid Approaches

Case studies of recent developments in hybrid governance show promise for this type of system. The European Union has begun integrating automated detection software with legal takedown requirements under its Digital Services Act, creating a hybrid system that combines technical monitoring with legal enforcement through a technically focused system (software) and an enforcement-based system (legal action). Another example is China's use of hybrid governance through its deep synthesis regulations, which require both the labelling of synthetic media and liability on behalf of the producer for any misuse[322] (both are regulatory requirements). The examples illustrate that hybrid models are not just

[321] Cyberspace Administration of China (n 65), WIPO (n 67).
[322] WIPO (n 67).

theoretical concepts but are currently in use around the world; however, the extent of their implementation and the way each jurisdiction uses them varies widely across jurisdictions.

Conclusion

The emergence of generative artificial intelligence serves to elucidate how intertwined copyright and cybersecurity are as domains[323]. What began as a debate about authorship and originality is morphing into a more comprehensive understanding that ownership disputes, gaps in liability, and enforcement mechanisms are all related to the stability of digital ecosystems. While copyright law protects human creative works, it is now faced with challenging outputs of this law's basic premise; meanwhile, cybersecurity laws must consider that, in some cases, legal ambiguity can be manipulated by attackers as an exploit vector[324] This chapter has illustrated that there is no unified global approach to addressing these issues: the European Union is pursuing an integral regulatory regime through proposals such as the AI and Digital Services Acts; the United States is relying on litigation and adversarial enforcement through existing legislation such as the DMCA; and China is implementing hybrid approaches that unite copyright enforcement with cybersecurity responsibilities, while India has been more cautious and has placed emphasis on human authorship, international organisations like WIPO have started the process of engaging in consultations with their member states to create some agreement; however, there is still no clear consensus on the matter[325].

There are, however, some areas in which there is more convergence among countries regarding their principles of how copyright applies: transparency of training dataset, accountability for results generated from the output and how the use of those results will not be misused[326]. The principles reflect an increasing understanding that copyright enforcement is not just protecting the rights of the creators but also has a direct impact on cybersecurity. This means that hybrid solutions which inject legal obligations (like Copyright) into technical protections (like Digital Rights) will ensure compliance from a normative standpoint (that is, the law needs to create a normative expectation of compliance with copyright) and from a technical standpoint [327] (that is, technology must incorporate and demonstrate in a verifiable manner compliance with copyright). Moreover, to achieve true accountability from AI created by humans, the myth of AI neutrality needs to be replaced with an understanding of AI accountability[328]. AI's creativity cannot exist without ownership and liability; rather, it will be necessary to govern AI using a framework that integrates law, technology, and ethics. This will allow for both innovations to flourish and for the resiliency of the digital ecosystem to be enhanced[329].

----------**********----------

[323] Zirpoli (n 2).
[324] Kedare (n 4).
[325] EU AI Act (n 49); Digital Services Act (n 49); DMCA (n 47); Cyberspace Administration of China (n 65); Muthu (n 8); WIPO (n 67).
[326] Giblin and Weatherall (n 41).
[327] Yang & Zhang (n 7).
[328] Samuelson (n 28).
[329] Guadamuz (n 27).

Chapter 14
The Economics of Cyber Resilience: Shifting from Technical Firewalls to Institutional Risk Management in India

Ayushi Gupta, B. Com, University of Delhi, M. Com Allahabad University

Abstract

Cybersecurity has been historically viewed as a technical problem in India—i.e., firewalls, malware scanners, intrusion detection systems, etc., were thought of as the primary means of defending against cyber threats[330]. However, due to the rapid growth of the digital economy (driven by Aadhaar, UPI, Fintech, digitisation and all of the other records of the artificial digital economy), there has come about a need for a shift in perspective regarding Cyber Resiliency. As such, this chapter argues that cyber resiliency should not only be considered a technology-based product but as an economic and institutional necessity[331].

This chapter discusses how cyber risk is viewed as an external systemic risk, i.e., a breach at one entity can create cascading impact on multiple entities across financial markets, supply chains, and critical infrastructures[332]. The chapter contrasts the extremely high costs for organizations due to data breaches (i.e., downtime, brand damage, regulator penalties, etc.) with comparatively lower investments made by parties to defend against such breaches (i.e., as cyber insurance, redundancy systems, and institutional governance frameworks)[333]. Finally, the chapter discusses specific Cyber Resiliency challenges faced within the Indian economy (e.g., limited resources available to deal with cybersecurity risks, the fact that breaches are frequently unreported, the limited number of skilled cybersecurity professionals available) while highlighting the necessity of developing and incorporating Cyber Resiliency processes and planning into future economic and policy-making initiatives[334].

As the foundation of resilience, Institutional risk management includes board-level accountability, mandatory disclosure norms, and recovery planning. The chapter evaluates regulatory frameworks such as SEBI's Cyber Security and Cyber Resilience Framework (CSCRF)[335], the Reserve Bank of India's (RBI) Banking Guidelines on Cyber Security[336], and the Crisis Management Protocols developed by CERT-In[337]. These frameworks are also compared with global models, including the European Union's NIS2 Directive[338] and the NIST Cyber Security Framework developed by the United States government[339].

---

[330] Palo Alto Networks, *The History of Firewalls* (2024).
[331] World Bank, *Cybersecurity as a Systemic Risk to Financial Stability* (2022).
[332] ibid
[333] Ponemon Institute, *Cost of a Data Breach Report 2023* (IBM Security, 2023).
[334] ibid
[335] Securities and Exchange Board of India (SEBI), *Cyber Security and Cyber Resilience Framework for Stock Exchanges, Depositories and Clearing Corporations* (2024).
[336] Reserve Bank of India, *Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices* (2023).
[337] Indian Computer Emergency Response Team (CERT-In), *Cyber Crisis Management Plan* (Government of India, 2022).
[338] Directive (EU) 2022/2555 (NIS2 Directive).
[339] National Institute of Standards and Technology (NIST), *Cybersecurity Framework 2.0* (US Department of Commerce, 2024).

The chapter is clear that resilience is not just about eliminating risk; it is about providing the ability to continue, adapt, and maintain trust in India's digital economy. Ultimately, the chapter argues that India must integrate cyber resilience into its governance and financial systems to ensure a future that is digitally enabled. Cybersecurity will be considered an institutional and economic challenge—as opposed to strictly a technical challenge. In doing so, India protects its digital transformation and creates an opportunity to become a global leader in resilient digital governance.

Keywords: *Cyber Resiliency, SEBI's Cyber Security, NIST Cyber Security Framework*

Introduction

In the digital age of India, now cyber resilience has become the most critical concept. It defined as the ability of institution to anticipate, recover from anticipated loss caused by cyber threats. Unlike traditional cybersecurity, which focus on providing protection through technical safeguards such as firewalls, antivirus software, hacks detention system and encryptions, cyber resilience recognizes that cyber-attacks may be occur in any institution in the future. It shifts the focus from solely defending against the cyber-attacks to ensuring continuity of the institutional operation, minimizing the economic losses and help institutional to adapt to an evolving threat ecosystem. In this way, resilience is not limited to technical protection, but it is about institutional capacity, accountability and systematic preparedness to address the anticipated cyber threats[340].

The difference between cyber security and cyber resilience is important. Cyber security primarily defensive in nature, aiming to block the unauthorized access and prevent the breaches through technical measures or we can say that traditional method. In contrast, cyber resilience is anticipatory and adaptive in nature, and it believes that no system or method can provide 100% security. Cyber resilience focusing on recovery speed, accountability and ability to absorb cyber shocks without affecting institutional continuity. This shift is very important in the modern digital age where critical infrastructure is digitally and well connected with financial system, supply chain, health care and national security. Therefore, a single cyber-attack can harm not only just one system but multiple interconnected system, leading to serious economic and operational loss[341].

From an economic point of view, cyber-attacks is not solely a technical problem, but systemic shocks that affect entire economy system. They disturb market, destabilize supply chain, break customer confidence, and impose heavy financial losses on both institution and government sector[342].

For Example, cyber-attacks can paralyze hospitals operations, while breaches in financial institutions can decrease the confidence of investors and trigger capital outflow. The economic sees cyber-attacks as an external sock that ripples across the economy, recuring institutional way to mitigate the impact. Cyber resilience is not a luxury but a necessity for safeguarding economic stability and national security for both institutions and the government[343].

---

[340] NIST (n 11)
[341] World Bank (n 4).
[342] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015).
[343] World Bank (n4).

As we observe, India is rapidly advancing towards becoming a 'Digital India'; consequently, we have become digitally dependent for a vast array of tasks. The most significant threat arising from this is the risk to our data privacy. We must recognize the gravity of the risk involved in storing all our personal information across numerous applications. This data security challenge cannot be resolved solely through technical measures—such as firewalls and antivirus software as many antivirus programs lack the necessary robustness to effectively shield users from hackers. In fact, many such programs merely create the illusion of providing protection. Furthermore, this is no longer merely a technical issue; it has evolved into a social issue where software alone is insufficient[344].

companies are setting aside funds meant for spotting threats before they strike. Not waiting until thin gs go live matters just as much as how money gets spent later. Funds once saved for emergencies no w shift toward early warnings and smarter defenses shaped during design phases[345].

Right now, India stands deep into a shift toward digital life - fueled fast by tools like Aadhaar, UPI, along with wider access to stock trading. Thanks to these steps, more people can reach banking services while systems run smoother, pushing India ahead on the world tech scene. Yet just beyond th at progress comes rising danger: fake messages pretending to be real, tricks played online, money co ns growing sharper every month[346].

India is getting better at dealing with cyber threats. The Reserve Bank of India has made rules for banks to follow when it comes to cybersecurity. These rules say that banks should think about the risks they face and have plans in place to deal with problems[347]. The Securities and Exchange Board of India is also working to make the financial markets safer.

The government of India is doing things like making a National Cybersecurity Policy and CERT-In is giving out guidelines to help organizations get ready.

- Even with all these things happening many organizations in India are still relying too much on things like firewalls to keep them safe. They are not paying attention to other important things like making sure they have good leaders and plans to manage risks. Indias organizations need to work to make sure they are safe, from cyber threats. The Reserve Bank of India and the Securities and Exchange Board of India are doing their part. Organizations need to do more to make themselves safe[348].

The Traditional Firewall Approach

The way we think about cybersecurity has been about using technical defences like firewalls, antivirus software and intrusion detection systems. These tools started in the 20th century when the main worry was people getting into networks without permission and bad code getting into systems. Firewalls help control traffic between networks we trust and ones we don't. Antivirus programs scan files and application to detect and remove malware from working and Intrusion detection systems watch network activity for suspicious patterns[349].

---

[344] Ponemon Institute (n 5).
[345] OECD (n 14).
[346] National Payments Corporation of India (NPCI), *UPI Annual Report* (2023).
[347] RBI (n 8)
[348] SEBI (n 7), RBI (n 8)
[349] Palo Alto Networks (n2)

This technical defence model assumes that threats come from outside and can be stopped with traditional approaches. The digital world has changed a lot. The rise of cloud computing, mobile devices and connected supply chains the lines around networks are blurry. This has made technical safeguards less effective and exposed institutions to new risks[350].

Limitations of the Technical Defence Paradigm

- Insider threats are a problem because they can easily get around the security measures that are in place to protect the organization. This is because people like employees and contractors already have access to the system. They can use this access to do things like leak important information or hurt the computer systems. Firewalls are not very good at stopping these kinds of threats because they cannot tell the difference between what's normal and what is not[351].

For example, phishing and social engineering attacks are very good at tricking people into doing things that can hurt the organization. These attacks focus on people not on the technology. If someone gets a phishing email that looks real, they might give away their login information. Download something bad. This means that the attackers can get around the security systems that're in place like firewalls and antivirus software. This shows that cybersecurity is not about having the right technology it is also about how people behave[352].

- Another problem is supplying chain attacks. These happen when organizations trust outside vendors and service providers much. Many organizations use software and hardware from companies, and they think it is safe. Sometimes attackers can compromise these suppliers and put bad code into their products. When the organization uses these products, they are putting themselves at risk without knowing it. The problem is that these threats come from people the organization trusts so the usual security tools, like firewalls often cannot detect them. Insider threats and supply chain attacks and phishing are all problems that organizations need to worry about[353].

- **Case Example**

2017, computers everywhere began locking up without warning. Because of a hidden flaw in Microsoft Windows, malicious code slipped through like smoke under a door. Instead of stopping it, firewalls stood idle while files vanished behind digital locks. Hospitals in the UK could not access patient records, trains halted, operations got delayed. Over 150 countries watched helplessly as machines froze one after another. Antivirus tools already installed made little difference when faced with something this fast. What looked secure yesterday failed completely by noon. Speed turned weakness into chaos before anyone could react.[354] Still firewalls matter but relying completely on it not enough. Antivirus software or traditional approaches not able to detect system hidden danger alone. People make

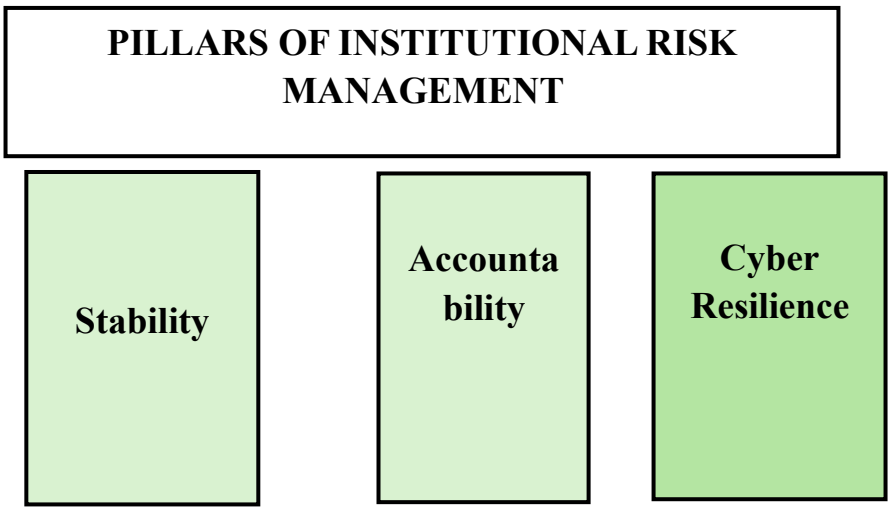
[350] Palo Alto Networks (n2)
[351] Ajay Biyani, 'Why Insider Threats Are Cybersecurity's Next Big Challenge' *Hindustan Times* (25 September 2024).
[352] Cybersecurity and Infrastructure Security Agency (CISA), *Avoiding Social Engineering and Phishing Attacks* (2021).
[353] CrowdStrike, 'What Is a Supply Chain Attack?' (2023).
[354] Cloudflare, 'What Was the WannaCry Ransomware Attack?' (2017).

mistakes. System gets compromised through suppliers too. WannaCry already showed how fast chaos spreads. all interconnected system gets blocked and not working. Strength comes not from blocking everything but staying upright after a hit. It can be done through proper planning, taking right decision, teaching and training team member on related problem. This builds real resistance[355].

Institutional Risk Management: A Paradigm Shift

Institutional risk management in the cyber sphere refer to top level management approach that focus on operational stability, accountability and systematic resilience instead of relying on technical approaches. Traditional approaches mainly focus on preventing attacks through firewall, antivirus security and encryption method. But institutional risk management assume that no system or method can provide 100% security[356]. Instead on focusing on technical method, this approach gives importance on institution stability through accept it that no system provides overall security, recover the losses and adapt it without compromising with their core functions. It recognises that cyber threats are not just a technical issue anymore, but it becomes systematic challenge. This risk has capacity to destabilise the financial market, digital payment system and critical interrelated infrastructure[357].

Institution risk management integrated with three most important pillars: -



Stability = continuity of operations, Accountability = board-level responsibility, Cyber Resilience = recovery and adaptation)

Board-Level Accountability

[355] OECD (n 14).
[356] ational Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations* (2018).
[357] World Economic Forum, *Global Risks Report 2024* (2024).

It's not just tech teams handling cyber resilience anymore. Directors now face growing pressure to manage digital threats through their duty to protect company interests. Setting long-term goals comes before funding decisions when preparing for destabilisation. Making cybersecurity part of broader risk systems becomes essential under this approach. Indian authorities like SEBI and RBI require top-level supervision, reflecting the shift of accountability to higher levels[358].

Risk Audits and Disclosure Standards

Start with clear checks on possible threats - those happen repeatedly - to keep institutions strong. When systems get reviewed, weak spots show up in how IT works, daily operations run, even in decision-making chains. Because of these reviews, people involved - like those who invest or oversee rules - learn what digital dangers exist. Openness like this doesn't just sit well - it earns confidence slowly over time. It also moves in step with standards seen elsewhere, including Europe's updated network safety rulebook. That framework pushes countries to demand full, timely reports when issues arise[359].

Planning for Incident Response and Recovery

Most of the time, strong systems survive because they know how to react when problems hit. Such blueprints lay out steps to spot trouble, limit damage, share details, then rebuild. What stands out is their focus on keeping things running - money flowing, hospitals working, power grids stable - even mid-cyberattack. A quiet force behind India's shield, CERT-In guides countrywide reactions[360]. At the same time, industry watchdogs require individual bodies to shape tailored bounce-back methods[361]. This method resembles the way, how companies top level management predict risks to protect future spending, keeping functions steady when uncertainty occur in the organisation.

India's Regulatory Frameworks

India set new rules for institution cyber resilience through regulatory framework that focuses on stability of operational function, accountability by top level management and resilience by taking appropriate mandatory framework.

SEBI's Cyber Security and Cyber Resilience Framework (CSCRF):

Now securities and Exchange Board of India make legal law that requires stock exchange, depositories and market intermediaries to adopt cyber resilience framework. These include well defined governance

[358] SEBI (n 7), RBI (n 8)
[359] NIS2 Directive (n 10)
[360] CERT (n 9)
[361] Gartner, *Incident Response Planning Best Practices* (2023).

and accountability structure, incident reporting and mandatory periodic auditing. This framework focuses on stabilized functioning of financial market, monitoring that cyber shocks can negative affect to investor confidence and systematic liquidity[362].

RBI's Guidelines for Banks

Reserve bank of India always makes rules and laws regarding the smooth functioning of banking system by making legal and strict laws. RBI holds main function regarding the stability of banks and services. RBI requires banks to implement board approved cyber security policies, conduct regular risk assessment, making incident response system. Updated guidelines to insure stabilize banking system and digital payment services it also helps to hold customer trust on Indian banking system[363].

CERT-In's Crisis Management Plans:

The main strategic framework of this plan is to prepare management for respond to and recover from cyber shocks and phishing attacks. The main aim of this plan is to minimize damage to critical infrastructure. Its key components involve identifying potential cyber crises and provide specific actions to stakeholders, focusing on that losses are minimised, and recovery is carried out effectively and efficiently[364].

In this sense, these frameworks can be regarded as a paradigm shift, since cyber resilience should be considered a matter of governance rather than just a technical problem[365].

The approach to managing risk on an institutional level represents a significant pivot of cyber-resilience in the country. India is incorporating governance, continuity and systemic resilience into its regulatory frameworks, moving beyond technical safeguards to being institutionally prepared by organisations having appropriate levels of accountability at the board level, performing risk audits and developing recovery plans that provide continuity for the organisation when experiencing a cyber event. Through the implementation of regulatory initiatives (SEBI, RBI and CERT-In), India is adopting best practices on a global level which will enable organisations to accept responsibility to adapt to, and recover from, cyber shocks while providing continuity of service[366].

As the digital economy in India continues to grow, institutional risk management will become increasingly important order to provide security for the financial markets, payment systems and critical infrastructure. Collectively, this shift is indicative of a greater understanding that resilience against cyber threats and vulnerabilities is a challenge beyond technical, but that cyber resilience is an economic and institutional necessity[367].

---

[362] SEBI (n 7)
[363] RBI (n 8)
[364] CERT (n 9)
[365] OECD (n 14).
[366] SEBI (n 7), RBI (n 8), CERT (n 9), NIS2 Directive (n 10).
[367] International Monetary Fund (IMF), *Cyber Risk and Financial Stability* (2021).

The Economics of Cyber Resilience

Cyber risk is both a technical challenge and an economic externality because incidents involving one firm produce consequences that can affect other firms—such as suppliers, customers, financial institutions, and even infrastructure on a national scale. For example, a ransomware attack targeting one hospital may disrupt care across multiple hospitals in the same region, while a payment gateway breach could undermine consumer trust and confidence in the entire digital ecosystem. Because of this interdependence, cyber resilience is an overall economic issue rather than one that only affects individual organizations[368].

Cyber Risk as an Economic Externality

As defined by economists, externalities represent costs or benefits incurred by individuals or parties (third parties) that did not participate directly in the transaction. Cyber incidents can be perfectly described as externalities because of how they expose many other companies to the risk of being harmed by someone else's attack due to their interconnectedness. Companies in the same supply chain expose all other companies within their supply chain to exposure from an attack if one of the companies in the supply chain has been attacked. Likewise, if one of the banks has an intrusion or is compromised it will diminish the public's trust and confidence in all other banks in the banking industry. In India, where UPI, Aadhaar and several fintech platforms connect hundreds of millions of users to the digital economy through their interconnectedness, this externality effect is compounded, thus it is important to view cyber resilience as a public good and invest accordingly through regulations and coordination[369].

Cost-Benefit Analysis of Resilience

Organizations typically compare the costs of investing in resilience to those that may result from a potential breach. Resilience investments include cyber insurance premiums, redundant backup systems, audit activity, and employee training. While these may seem burdensome to micro, small, and medium-sized enterprises (MSMEs); the costs associated with economic losses due to breaches—such as downtime, reputational damage, regulatory fines and customer attrition—far exceed these amounts[370].

For example, downtime resulting from a digital payment system outage can effectively bring retail transactions to a halt across the country. A single day's outage of the UPI system could mean billions of rupees in lost commerce. Therefore, from a cost versus benefit viewpoint, spending on resilience is not a 'nice to have'; it's a 'must have'. The challenge is quantifying those risks so that SMBs have incentive to invest in them before a breach occurs (rather than reactively)[371].

---

[368] IMF (n 39)
[369] World Bank, *Cybersecurity as a Systemic Risk to Financial Stability* (2022).
[370] Ponemon Institute (n 5).
[371] NPCI (n 18)

Cyber Insurance as a Financial Instrument

Cyber insurance is becoming a popular way to manage your financial risk throughout the world. In India, however, we are facing challenges related to its adoption as an insurance solution.

- **Actuarial Data:** Insurers in India have difficulty in pricing their cyber insurance policies because of insufficient historical data on cyber incidents[372].
- **Affordability:** Small to medium-sized businesses (MSMEs) typically operate on very narrow margins, making it cost-prohibitive for them to purchase cyber insurance premiums[373].
- **Awareness Gap:** Many businesses still look at cyber-risk as a technology issue instead of a financial issue in their risk management strategy[374].

Bringing together these facts, implementing a way to facilitate rural economic resilience using cyber insurance has the potential to become a very valuable financial tool for organizations. In addition to spreading the financial risk to different organizations in a region, cyber insurance creates a financial buffer to recover from catastrophic losses, while also providing incentives to organizations for implementing risk mitigation practices. Policymakers can promote the adoption of cyber insurance products through subsidies, tax incentives or regulatory mandates for all organizations, but especially for organizations operating in critical industry sectors such as banking and healthcare[375].

Economic Resilience Tools

Apart from insurance there are different ways of employing Economic Resilience Mechanisms listed below that will enhance a company's ability to withstand attack and recover from disaster.

Public-Private Partnership: To reduce the asymmetry of information, organizations need to share Cyber Risk Threat intelligence. Examples include the Government of India's Cyber Emergency Response Team, (CERT-In)[376]; Additional cooperation with Industry Associations by Gov't can provide additional preparedness.

Investment in Redundancy: Organizations should invest in backups, Disaster Recovery sites and cloud-based continuity of operations failover facilities. Although initially expensive, they will result in fewer losses when a company experiences an attack[377].

Regulatory Frameworks: The SEBI and the Reserve Bank of India (RBI) are embedding Cyber Resilience in their Rules and Regulations Se Teil 8020 et al to make it a requirement of doing business, or as a required component of doing business to be compliant as an organization, as opposed to optional[378].

---

[372] Insurance Regulatory and Development Authority of India (IRDAI), *Report on Cyber Insurance in India* (2022).
[373] IRDAI (n 44)
[374] IRDAI (n 44)
[375] OECD, *Insurance and Risk Management for Cyber Resilience* (2021).
[376] CERT (n 9)
[377] Gartner (n 33)
[378] SEBI (n 7), RBI (n 8)

Case Study: UPI's Resilience Planning

This is the case study of a financial system that is functioning well and providing a reliable service for millions of people every day. It is a vital component of India's digital payment system (Unified Payments Interface - UPI) and processes billions of transactions each month. A failure of the UPI payment system would have serious and numerous negative implications throughout India's economy[379].

To prevent system failures, the UPI has taken extensive measures to ensure that:

- Its operational systems are designed with redundancy and backup systems that support uninterrupted operation.
- Real-time system monitoring and management to detect any anomalies or problems before they become critical.
- Developing and implementing incident response procedures that will allow the UPI to quickly restore service in the event of a security breach or incident.

The successful implementation of these resilience investment plans has helped UPI maintain consumer trust in its service and allowed UPI to remain an active participant in the growth of India's digital economy despite increasing threats from cybercrime. As demonstrated by the UPI case study, investing in resilience benefits individual organizations; it benefits the entire economy[380].

1. India-Specific Challenges

India's progress towards improving its Cyber Resilience has been faced with certain unique challenges due to the Country's Economic Structure, Regulatory Framework, and Organizational Culture. Although there has been significant progress made in Digital Transformation, vulnerabilities still prevent the successful implementation of Resilience Strategies[381].

Micro Small and Medium Enterprises (MSME's) do not have the funds available for Resilience: MSME's are the Heart and Soul of the Indian Economy (30% of GDP, with millions of Employees), however, MSME's are operating on Tight Margins and Having Limited Budgets. As such, investing in Cyber Resilience (Insurance, Audits, Security Devices, etc.) is viewed as a Luxury, rather than a Necessity. Most MSME's are using Old Technology, Have Limited Full Time IT Personnel, and are Very Dependent on Third Party Service Providers; several of these factors contribute to the Issue of Supply Chain Risk. The Affordability Gap in Cyber Insurance compounds this issue leaving MSME's Vulnerable to the Financial Impacts associated with Breaches. The issue creates a Systemic Risk given the Deep Integration of MSME's into Larger Supply Chains since one Breach will create multiple impacts across Industries[382].

---

[379] NPCI (n 18)
[380] NPCI (n 18)
[381] Ministry of Electronics and Information Technology (MeitY), *National Cyber Security Strategy Draft* (2021).
[382] Federation of Indian Chambers of Commerce and Industry (FICCI), *Cybersecurity Challenges for MSMEs in India* (2022).

2. Underreporting of Breaches Weakens Collective Defence

There is a long-standing problem of organizations failing to report cyber incidents due to fear of damaging their reputation, incurring regulatory scrutiny, or losing customer trust. This lack of a reporting culture hinders the sharing of threat intelligence, which contributes to the overall lack of effective collective defence mechanisms. Additionally, without reporting of breaches, regulators and policymakers cannot access the data necessary to assess systemic vulnerabilities or create effective interventions. Lastly, without a culture of strong disclosure, corporations are unable to learn from one another's experiences, resulting in a cycle of unpreparedness. As exemplified by global frameworks such as the EU's NIS2 Directive, this highlights the need for India to strengthen enforcement pertaining to mandatory reporting of incident breaches[383].

3. Shortage of Skilled Cybersecurity Professionals

Cybersecurity Professional Shortage India has a remarkably large talent gap in cybersecurity. While the country has a significant pool of IT graduates, it has very few specializing in area such as threat intelligence, incident response, and resilience planning. Most qualified cybersecurity professionals are further concentrated in metropolitan areas, causing those working in small cities or rural enterprises to be left without ample support. There is significant market demand for qualified cybersecurity professionals, which continues to greatly exceed supply; therefore, many micro-, small-, and medium-sized enterprises (MSMEs) and others are faced with increasing challenges when trying to hire highly qualified staff. The gap in the regulatory frameworks has left government agencies and regulators unaffected by the potential implications of this continuing problem and, therefore, limits their ability to monitor compliance and have effective responses in the event of a crisis. To bridge this gap, significant investment in specialised training programs, industry-academia partnerships and economic incentives to attract and retain talent within the country will be required[384].

4. Policy Enforcement Gaps Despite Strong Frameworks

Despite the existence of strong policy frameworks, there remain numerous gaps between the design of regulatory frameworks and their enforcement. This is true for many of India's regulatory bodies, including the Reserve Bank of India (RBI)'s Cybersecurity Guidelines for Banks, the Securities and Exchange Board of India (SEBI)'s Cyber Security and Cyber Resilience Framework (CSCRF) and CERT-In's Crisis Management Protocols. Specifically, the lack of adequate resources and penalties for non-compliance create an environment where regulatory authorities cannot fully audit and assess compliance. Consequently, many companies view compliance as a "checkbox" exercise rather than incorporating resilience into their operational culture, and the lack of consistent enforcement of existing laws perpetuates an ineffective regulatory framework[385].

---

[383] NIS2 Directive (n 10)
[384] NASSCOM, *Cybersecurity Talent Report India* (2023).
[385] SEBI (n 7), RBI (n 8), CERT (n 9).

5. Cultural Challenge: Cyber Risk as an IT Issue, not a Business Continuity Issue

The issue of cyber risk being perceived as an IT issue rather than a business continuity issue is likely the most significant obstacle facing organisations in India. Many Indian companies still perceive cyber risk solely as an IT-related issue, and therefore, the responsibility for managing that risk lies exclusively with their IT departments, instead of being viewed as a strategic issue that requires oversight from the board. The limited perspective encourages lack of investment into resilience preparation as well as ignoring continuity strategies. Building cyber resilience requires adopting an integrated viewpoint across governance, risk management and operational continuity but organizational inertia frequently inhibits organizations from undertaking the necessary change. Until organizations develop a true understanding of the notion that cyber risk falls within the umbrella of business continuity risk; they are always going to be reactive to cyber resilience rather than proactive[386].

Policy Recommendations

India's fast-paced digital development is why Internet Safety is one of the highest priorities on the National to-do list. SEBI's CSCRF has improved Security for Financial Services but there are many other Industries like Manufacturing, Health, Energy, and Transport where Cyber Crime is just as much of a threat as it is in the Financial Industry[387].

Here are some Policy ideas to increase Cyber Resilience in India:

1.Expanding SEBI's CSCRF Principles Beyond Finance

SEBI has very Strong Corporate Governance Processes for Financial Services (CSCRF) however, Security Processes in other industries could benefit from Corporate Governance Processes like CSCRF so that management will be accountable for ensuring that they have completed a Risk Assessments for their Organization and created a Security Resilience Plan for their Business. By normalizing Security Processes for all Industries, the Government will create very Good Security Practices for All of our Nation's Businesses and make it much easier for the Government Agencies involved to Develop and Execute a National Response to Cyber Crime[388].

2.Incentivizing Cyber Insurance Adoption

Cyber Insurance currently does not exist in a way that organizations find affordable. Therefore, we recommend to government officials to create incentives such as Tax Benefits for Cyber Insurance, Premium Subsidies for Qualified and Registered MSMEs, and Startup a Financial Risk Pool where Private Insurance Companies Pool Risks from Public and Private Sector Organizations into one combined Financial Risk Pool. Organizations can reduce the financial damage caused by cyber-attacks by implementing cyber insurance as part of their overall financial risk management while enabling the

---

[386] PwC India, *Cyber Risk as Business Continuity Risk* (2022).
[387] MeitY (n 29).
[388] SEBI (n 7).

insurer to create systemic resilience via the data collected and the industry standards that are created. This will also lead to greater transparency since insured organizations will typically be more willing to report incidents, they experience to meet the policy requirements[389].

3. Building MSME Capacity Through Subsidies and Shared Platforms

MSME Capacity Building Through Subsidy and Shared Platforms Micro, small, and medium enterprises (MSMEs) are the foundation of India's economy yet remain constrained in their ability to build resilient organizations. By providing government-funded subsidies for basic cybersecurity tools, shared resilience platforms (e.g., cloud-based backup and monitoring), and additional training programs, this gap can be closed. A framework based on a collective resilience model that allows MSMEs to pool resources (e.g., intelligence sharing) to protect themselves from threats and build redundancy would have a positive impact on reducing costs and increasing systemic protection through economies of scale. The approach will be like other cooperative models created in agriculture and finance but adapted for the digital economy[390].

4. Mandating Breach Disclosure to Strengthen Systemic Awareness

Creating Systemic Awareness Through Mandated Breach Disclosures The underreporting of breaches is one of the most significant weaknesses in India's cyber ecosystem. The implementation of mandatory breach disclosures and legal protections against potential reputational harm will create greater systemic awareness and allow for a quicker and more efficient response collectively. Disclosures from companies should be differentially tiered: minor incidents reported to the regulator; major breaches reported publicly to strike a balance between openness and practicality. Being collectively accountable through building sustained collabouration will create an environment where being resilient as opposed to being at a competitive disadvantage is just as important to everyone as it is for those who actively work on their own transformation efforts[391].

5. Fostering Public-Private Partnerships for Intelligence Sharing

Fostering Public-Private Partnerships for Joint Intelligence Sharing The pace of change in cyber threats far exceeds the speed of regulatory change. Thus, sharing intelligence between the public and the private sector is necessary. A public-private partnership (PPP) provides a forum to establish an institutionalized form of collabouration among government, industry associations, and private firms. There will be collabourative platforms established for sharing real-time threat intelligence, coordinating responses to incidents, and providing joint training and exercise opportunities. This will also allow the development of public-private partnerships with universities and research entities so that India can develop the homegrown skills to model cyber risks and the technology solutions required for enhancing resilience[392].

---

[389] OECD (n 47)
[390] Confederation of Indian Industry (CII), Building Cybersecurity Capacity for MSMEs in India (2022).
[391] NIS2 Directive (n 10)
[392] WEF (n 29).

6. Integrating Cyber Resilience into National Economic Planning

Integrating Cyber Resilience into National Economic Risks Cycles India must embed cybersecurity within its overall monetary policy. Just as physical risk has been incorporated into infrastructure policy, so too must cyber risk be factored into the digital infrastructure public policy. In addition to allocating a line item for growth resilience in national economic policy, all national macroeconomic forecasts must embed cyber risk in making estimates of GDP; and resilience must be treated as public good. As a result, India's digital growth will match up with systemic health and innovation will not be compromised by the risk of being vulnerable[393].

Conclusion

The evolution of India's digital economy has proven that relying solely on traditional technical firewalls and perimeter defences is insufficient to address the systemic and interconnected risks facing the current threat landscape. While technical security controls (firewalls, antivirus software, and intrusion prevention systems) are still critical to protecting our systems, they are no longer adequate to address the increasing prevalence of cyber threats and the way in which they are intertwined with one another. There needs to be a transition towards using institutional risk management (as opposed to solely technical security) to build resilience into governance, policy, and finance[394]. This approach recognizes that cyber threats are not only technical disruptions but can also result in economic losses that will destabilize markets, supply chains, and critical infrastructure. Cyber resilience will be a fundamental component of India's digital economy. The costs associated with cyber incidents (financial losses, lost productivity, reputational harm, and regulatory penalties) far exceed the investments required to develop public's confidence and to continue to allow for the ongoing adoption of India's digital economy, particularly considering the rapid digitization that has occurred (Aadhaar, UPI, and fintech growth)[395]. By treating cyber risk as an externality to the economy, India is acknowledging that the vulnerability of one organization can have a cascading effect across multiple sectors and lead to systemic fragility throughout the economy. As such, resilience will be a shared responsibility that will require coordinated efforts among regulators, industries, and businesses[396].systems that can remain resilient over time[397]. Resilient systems are essential to maintain the

It is critical to note that there is no perfect way to completely reduce risk - resilience is rooted in ensuring some degree of continuity, rapid recovery and adaptability. The objective of resilience is to ensure that vital functions – such as financial transactions, delivery of healthcare services, provision of energy, and protection or performance of government functions – can continue to operate, notwithstanding their potential disruption because of an event[398]. The fundamental purpose of building resilience is to shift the mode of cyber risk management from being reactive to pro-active.

---

[393] IMF (n 39).
[394] National Institute of Standards and Technology (NIST), *Cybersecurity Framework 2.0 Draft* (2023).
[395] NPCI (n 18)
[396] IMF (n 39), NPCI (n 18)
[397] IBM Security, *Cost of a Data Breach Report* (2023).
[398] OECD (n 14).

Organizations need to develop the processes and capabilities to anticipate, absorb and recover from external shocks while maintaining their long-term viability[399].

To enable the future growth of the digital economy in India, it will be essential to build resilience into India's institutional fabric. This will entail developing systems that embed resilience into governance structures and regulatory and financial instruments, such as board-level accountability, cyber insurance, etc[400]. At the same time, it will be necessary to help the micro, small and medium enterprises (MSMEs), which constitute the mainstay of the Indian economy, through the provision of subsidies, shared resilience platforms and training for them to build up their resource capacity[401]. Furthermore, India will need to develop stronger standards for breach disclosure and promote intelligence-sharing and public-private partnerships, as well as work towards achieving alignment with other international standards of resilience. By institutionalizing resilience[402], India will protect its digital transformation, as well as position itself as a global leader in the development of economic security standards for the digital age[403].

To build India's digital future, we need to focus on solidifying the fundamentals of continuous service delivery, rather than creating large barriers to entry. The country must prioritize cyber resiliency at a national economic level, which includes embedding it throughout government, policy and financial systems. By making resilience the foundation of India's digital initiative, we can turn weaknesses into strength, providing an ever-larger, more flexible, and globally competitive digital economy that can withstand changing cyber threats[404].

----------**********----------

[399] Gartner (n 33)
[400] SEBI (n 7), IRDAI (n 44).
[401] FICCI (n 54), CII (n 62).
[402] NIS2 Directive (n 10), WEF (n 29).
[403] World Bank, *Cybersecurity as a Public Good* (2022).
[404] IMF (n 39).

Chapter 15

Artificial Intelligence and Cyber Risks: Legal Challenges and Regulatory Responses in the Digital Age

Deep Mahata, Student of LLB (H), Department of Legal Studies, Swami Vivekananda University

Abstract

Artificial intelligence is increasingly becoming a major force in shaping the landscape of the digital world, offering many prospects as well as creating many obstacles in the field of cybersecurity. In this paper, the role played by AI technology will be analyzed in terms of both its benefits and risks. First of all, artificial intelligence helps in increasing efficiency in threat detection and response while contributing to better overall security measures. At the same time, the potential of AI to be used for conducting attacks on cybersecurity systems is becoming increasingly real.

The paper considers the legal issues that have emerged due to these AI-based cyber threats. It is becoming increasingly challenging to resolve these legal issues in light of current laws due to their tendency to trail far behind technological advances. Moreover, the absence of any legislation related to the usage of AI technology has become another obstacle in the way of proper risk management.

Also, this paper will consider the contemporary approach to managing cybersecurity risks at both national and global level and will emphasize that the creation of new instruments of law that could be easily adapted to new circumstances was crucial. Also, the significance of ethics in overcoming current problems will be underlined.

To conduct a balanced analysis of this problem, an interdisciplinary research strategy is employed here, which takes into account both technological factors and legal issues. Finally, it should be said that addressing cyber security risks linked to AI requires not only strict law and innovations but also morality.

Keywords: *Artificial Intelligence (AI), Cybersecurity, Legal Challenges, AI-based Cyber Threats, Ethics & Risk Management*

Introduction – Artificial Intelligence and Emerging Cyber Risks

Artificial intelligence (AI) is one of the technologies that have had a significant impact on the digital world, forming an integral part of modern life. The implementation of artificial intelligence through task automation and decision-making processes has made many operations much more efficient, thus taking an active part in various fields, including cybersecurity, enabling faster identification of threats and preparing for tackling any issues. However, despite being one of the best ways to ensure security of information resources, it has created new challenges in the sphere of cybersecurity.[405]

Among the topmost concerns which should be addressed are those of the two-way abilities of AI. While on one hand AI helps in improving cybersecurity, on the other hand it can be misused for wrong

[405] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021).

purposes. There have been reports of cybercriminals resorting to the use of AI to initiate sophisticated attacks, which include automated hacks, deep fake-enabled identity thefts, and customized phishing operations. Such AI-powered attacks prove to be very challenging to combat since they tend to adapt and evolve rapidly.

In addition, the increasing use of artificial intelligence (AI) poses important issues relating to accountability and liability. In cases where the use of the AI system results in any kind of damage either due to a breach of security or the result of any deliberate tampering, it may become challenging to assign responsibility. Should the responsibility lie with the developer, the end-user, or the organization using the AI technology? This is a problem that hasn't been sufficiently regulated by current legislation.[406]

Moreover, the constant development and progress of AI systems create a number of challenges for regulation of AI technologies. Conventional cybersecurity legislation generally takes on a reactive and fixed form, while the risk generated by AI technologies is both proactive and continuously evolving. The difference in approaches creates a gap in regulations, making the system highly susceptible to exploitation. It is essential to develop laws that can evolve with technology.[407]

In this chapter, the reader is introduced to the complex interplay between artificial intelligence and cybersecurity. Not only does the chapter point out the promising role played by artificial intelligence in enhancing digital security but it also emphasizes the risks associated with its use. What makes the chapter more intriguing is its emphasis on the need for novel laws and regulations to manage artificial intelligence within the digital space.[408]

Nature and Types of AI-Based Cyber Threats

AI has drastically altered the way cyber threats function and increased their complexity and adaptability to make them much harder to recognize than ever before. While classic attacks require a specific approach to be executed, AI technologies allow cyber threats to run independently and change tactics depending on the current conditions and data gathered in the process. This development introduced the emergence of the new breed of cyber dangers that poses a threat both to our technological infrastructure and laws currently in effect.[409]

The first and foremost example of cyber threats generated by means of AI would be deepfake technologies that employ artificial intelligence to create convincing audio or video content that cannot be easily distinguished from the original. Such cyber threats may be used for various purposes including personal identity theft, fraud schemes, manipulation, or defamation. For example, a maliciously edited recording or video of a person may be quickly disseminated among the masses before anyone realizes that it is not authentic.[410]

A further issue of note is the development of AI-based malware. Different from regular malware, which executes pre-programmed actions, AI-powered malware changes its course based on what happens

---

[406] European Commission, Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act) COM(2021) 206 final.
[407] World Economic Forum, Global Risks Report 2023 (2023).
[408] United Nations, Report of the Secretary-General on Digital Cooperation (2019).
[409] European Union Agency for Cybersecurity, Threat Landscape for Artificial Intelligence (2021).
[410] National Institute of Standards and Technology, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (2019).

around it, making it capable of adapting and modifying its tactics in response to the situation it encounters in order to evade security solutions. In addition, the malware itself decides the best way to proceed in an attack, thus making such malware more hazardous as it will be able to penetrate through any security measures used.

Finally, the issue of automated vulnerability scanning needs mentioning in terms of the dangers posed by AI. On one hand, cybersecurity experts can employ AI technologies to scan vulnerable parts in systems and fix them before the hackers have a chance to do anything; however, on the other hand, AI technologies enable cybercriminals to scan huge networks and find entry points in the shortest possible time.

The evolution of social engineering tactics in conjunction with AI has also taken place. Typically, the attacks were based on simple methods involving deception and, in particular, phishing emails. Modern AI technologies enable hackers to create highly targeted, personalized, and effective communications based on analysis of a victim's online activities, interests, and communication habits. Such intelligent phishing technology can write convincingly mimicking certain styles and producing targeted communications.[411]

It is vital to emphasize that AI is a useful tool not only for hackers but also for cybercrime fighters. AI technologies are extensively applied in cybersecurity practices to detect threats, analyze anomalies, and operate automated response systems. It provides an ability to process huge amounts of data quickly and to react promptly to suspicious behavior.[412]

Nonetheless, the ability of AI to protect against cyber threats also raises concerns due to its dual capabilities. In other words, the technology capable of protecting the network from cyberattacks can simultaneously be employed to conduct an attack. Therefore, defining the boundaries between legal and illegal applications of AI becomes complicated.

Moreover, the dynamic nature of AI cyber threats poses major difficulties for the law enforcement system. Typically, legislative measures and regulations are aimed at controlling static cyber threats, which are easily identifiable and classified under certain categories. In contrast, AI cyber threats are characterized by their dynamicity and flexibility. In addition, some AI cyber threats may act autonomously, meaning that there will be no person to take responsibility for any negative consequences.

To sum up, the emergence of AI-based cyber threats adds another layer to contemporary cybersecurity issues. Notably, the nature of such threats and their types call for specific measures in dealing with AI cyber threats.[413]

Legal Challenges in Regulating AI and Cyber Risks

The development of Artificial Intelligence technology has led to a number of legal issues that cannot be easily solved using the existing systems of laws. Even though artificial intelligence promises many advantages, it has its fair share of problems that cannot be ignored in fields such as responsibility,

[411] Kaspersky, Spam and Phishing in 2021 (2022).
[412] IBM, IBM Security: AI in Cybersecurity Report (2021).
[413] World Economic Forum, Global Risks Report 2023 (2023).

privacy, and legal authority. Since the law is meant to guide humans, it is faced with the challenge of adapting to this new reality of machine decisions.

Another significant problem is that of accountability. In the case where the AI makes its own decisions, detects a threat, or takes action, it can be hard to determine who is liable for any mistake that occurs. For example, if an AI-driven cyber security software program does not succeed in stopping an attack or even causes one, whose fault would it be? Who will be accountable for any failure—a person who programmed the software, the company who implemented it, or the individual who trusted it? The current laws cannot easily be applied to autonomous machines.[414]

The other important problem that arises in connection with this type of technology is that related to data protection. It involves huge quantities of data that must be used for the purpose of successful work of the artificial intelligence. Personal data is involved, creating problems related to violation of personal rights as well as potential abuse. Some attempts have been made to solve the problem by means of such measures as data minimisation, consent, as well as right to explanation. Nevertheless, these laws were not initially designed for AI technologies, and as a result of this, they do not take into account such issues as algorithmic bias, black box decision-making, and huge amounts of data processing.[415]

Another important problem in terms of law related to AI and cyber security is that related to jurisdiction. The nature of cyberattacks makes it rather hard to identify the jurisdiction applicable to the case, as it usually spans across several jurisdictions at once. It is possible that an AI-based cyberattack can be launched from one country while victims belong to another and use servers of third parties.

Another aspect which further complicates the issue under discussion is the absence of a single set of unified legal norms on how to regulate the use of AI technologies. Although some legislative frameworks in various countries and regions start being developed, there is no internationally recognized legal act that could guide the activities related to the use of AI.[416]

In addition, the ever-changing character of the technologies used poses another significant challenge as laws tend to be quickly outdated in this case. In other words, unlike traditional problems discussed in courtrooms and addressed by legislators, artificial intelligence and all of its implications should be regulated much more flexibly.

Summarizing everything said above, it should be stated that the issue of AI and the legal regulation of this technology is rather complicated and needs thorough discussion and cooperation on both national and international levels. The aspects of liability, cyber risks and data protection mentioned above illustrate perfectly the problems that arise from the current legal practices.[417]

National and International Regulatory Responses

In the process of advancing and embedding itself within people's lives, there have been efforts from many governments around the world to acknowledge the dire need for regulatory measures on the use

[414] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2021).
[415] General Data Protection Regulation, Regulation (EU) 2016/679.
[416] Organisation for Economic Co-operation and Development, OECD Principles on Artificial Intelligence (2019).
[417] United Nations, Report of the Secretary-General on Digital Cooperation (2019).

of Artificial Intelligence technology. It is not anymore an idea of the future; rather, it is impacting the economy, the form of governance, and even the cyber security framework.[418]

On a national scale, many nations have developed AI policies and cybersecurity strategies designed to foster innovation yet protect the public's interest. For instance, most countries' policies involve developing initiatives that encourage innovation and the development of digital infrastructure and ensure that there is no misuse of AI technologies. Many nations are now increasingly engaging in cybersecurity practices that utilize AI capabilities to mitigate security threats. Some nations have already started working on developing regulations concerning certain areas such as data protection and algorithms.[419]

Nevertheless, each country employs its own methods of regulating artificial intelligence. There are those who value progress, which means that they have adopted a lenient regulation system where the development of technology is not impeded in any way. Then there are those who prefer a cautionary attitude, putting their emphasis on the protection of personal information and ethics. Each method has its own merits, but their differences may become a problem for international collabouration.[420]

Internationally speaking, institutions have been instrumental in establishing guidelines regarding the issue. The United Nations and the Organisation for Economic Co-operation and Development have devised various ethical principles for the use of artificial intelligence in different fields. These guidelines stress the importance of transparency, accountability, fairness, respect for human rights, and other such factors. Although they are non-binding recommendations, these ethical guidelines may be considered when a country establishes its own regulations.

Despite all the mentioned actions, one of the most difficult obstacles in regulating AI is the absence of universal norms on an international scale. At the moment, there is no unified set of international legal standards that could control the use of AI technologies. The process of regulating AI technologies takes place in a fragmented way, when each country develops its own norms. Such regulation leads to uncertainties that could become obstacles to the activities of multinationals that work on an international scale. Additionally, such regulation complicates resolving cross-border issues like cybercrime or misuse of technologies. Another essential point that requires attention is the need for international cooperation. Since cyber risks related to AI are not limited to any territory, their isolation and separate regulation do not solve the problem.[421]

Alongside harmonization, the need for adaptability and flexibility of regulation becomes increasingly more obvious too. Technologies are dynamic and rapid changes within the realm of AI require an equally agile response from the legislative branch, lest they find themselves outmoded very soon. It is therefore vital to develop regulatory methods that are able to cope with technology and its constant changes in time. For instance, soft law instruments and regulatory sandboxes might prove useful in such cases.[422]

It would be fair to conclude that considerable progress has been achieved in tackling the problem of AI on both domestic and international scales. However, there is still a long way ahead of us towards solving this problem once and for all. As of now, one of the major drawbacks in AI regulation is its

---

[418] World Economic Forum, Global Risks Report 2023 (2023).
[419] NITI Aayog, National Strategy for Artificial Intelligence (2018).
[420] European Commission, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust COM(2020) 65 final.
[421] Council of Europe, Convention on Cybercrime (Budapest Convention) (2001).
[422] Financial Conduct Authority, Regulatory Sandbox Lessons Learned Report (2017).

inconsistency and multiplicity, which makes it difficult to control. What should be done to solve this problem? Harmonization of laws and cooperation between countries seems to be the key.

Ethical Dimensions and Risk Management in AI Cybersecurity

Now that Artificial Intelligence is being deeply integrated into cybersecurity, it is time for the significance of ethics not to be underestimated. Although law creates an enabling framework for any activity and serves as its basis, ethics makes sure that whatever technology gets implemented is done so ethically and is based on certain standards that correspond to human values and human rights. Ethics plays the role of a compass within the sphere of AI-based cybersecurity.[423]

Another critical issue that arises in relation to ethics and artificial intelligence (AI) is the problem of algorithmic bias. AI is trained based on the information that exists in the dataset, and if there are any biases present in the data, then the predictions made by the algorithm will also be skewed. For instance, when it comes to the domain of cybersecurity, there can be instances where the threat posed to users is not properly evaluated, which might lead to the unjustified targeting of some individuals.

Transparency is yet another crucial ethical value. Many AI applications operate on a "black box" basis, which means that their decision-making process involves sophisticated mechanisms whose workings cannot be fully comprehended by people. In cybersecurity, this can become problematic if organizations find themselves incapable of elucidating the reasoning behind their decisions, such as identifying an emerging threat or choosing a particular course of action. It becomes particularly relevant if the decisions made by the organization have serious implications, including denying entry, labeling individuals, or dealing with cyber attacks.[424]

The issue of accountability in itself raises a vital point. As mentioned in previous sections of the book, it may prove challenging to define who should be held responsible for the activities performed by artificial intelligence. Ethical guidelines try to resolve this problem through highlighting the significance of having humans in charge. Regardless of how independent a particular algorithm might seem, there should always be ways to hold humans accountable for its decisions and actions.

A number of ethical frameworks designed by different organizations emphasize such concepts as accountability, responsibility, fairness, and human supervision. The purpose of promoting these approaches is to promote responsible innovation while developing new technologies. This way, innovations can help people without compromising their fundamental rights and well-being. Cybersecurity technologies, in turn, need to be created to protect personal information and ensure that no harm is done to any party involved.

Aside from ethics, risk management becomes crucial in combating AI-driven cyberattacks. Companies should become proactive in dealing with such threats by recognizing, assessing, and controlling any risk at an early stage. The first thing for companies to do is to establish a strong cybersecurity strategy that makes proper use of AI technologies. It includes safe design, timely risk identification through assessment, and appropriate access controls.[425]

---

[423] United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence (2021).

[424] Royal Society, Explainable AI: The Basics (2019).

[425] International Organization for Standardization, ISO/IEC 27001 Information Security Management Systems (2013).

Monitoring also becomes necessary for companies dealing with risks associated with AI technologies. Since these technologies work under dynamic conditions, risks may emerge quickly and require fast actions to be undertaken. Thus, continuous monitoring helps companies stay aware of what happens within the system and react to the problems in time.[426]

The inclusion of ethical principles in the development of AI also needs to be considered. Known as 'ethics by design', it allows embedding ethical principles right in the process of the development of the technology and, hence, developing a system that would be not only effective but also responsible.

Finally, when dealing with cyber risks associated with AI technologies, it is necessary to find a balance between legal and ethical approaches. Whereas legal frameworks define what behaviour is not acceptable and outline basic rules, ethics goes further and encourages fair and honest actions in addition to merely complying with the law. As seen from above, a purely legal strategy cannot solve all issues related to AI in cybersecurity, while ethics allows having an even broader perspective on the matter.[427]

To conclude, ethics plays an important role in AI in cybersecurity just like any other aspect under discussion. Bias, transparency, accountability, among others, should definitely be taken into consideration when addressing ethical questions in relation to AI in cybersecurity. In addition to that, risk management is of critical importance for ensuring cyber safety as well.

Future Directions and Conclusion – Towards a Resilient Legal Framework

In view of the ever-evolving nature of AI technologies, the future of cybersecurity legislation and policy regulation is going to be highly dependent on how efficiently legal institutions are able to keep up with these changes. Current laws, which have been tailored to a much less dynamic environment, will continue to prove themselves incapable of dealing with the problems that have arisen. Thus, the need for creating new laws and frameworks becomes inevitable.[428]

A major step to take in order to ensure success for the future is the creation of laws that are technology-neutral. In other words, laws should concentrate on addressing the problem itself rather than some particular type of technology being involved. The idea is that these laws should be able to maintain their relevance despite any rapid development of technology. Due to the fact that AI technologies are currently developing rapidly, laws may lose their value quickly if they are focused on addressing certain issues associated with a certain technology.

On the other hand, issues relating to accountability cannot be ignored. As AI becomes more and more autonomous, questions relating to responsibility and liability will be of growing importance. Future laws on the use of AI will need to address these questions by setting out clear rules on who will be responsible in what situations, as well as procedures for oversight, auditing, and redress. Without such clarity, AI technology will not be trusted, thereby limiting its usefulness.

The role of judicial interpretation in relation to AI and cybersecurity will be of increasing importance in years to come. Courts will have to interpret existing laws in light of emerging technologies, especially in areas where the legislature has not made any provision. The rulings of the courts will be

[426] National Institute of Standards and Technology, AI Risk Management Framework (2023).
[427] European Union Agency for Cybersecurity, Cybersecurity and AI: Opportunities and Challenges (2021).
[428] World Economic Forum, Global Risks Report 2023 (2023).

significant for filling legal gaps, as well as developing legal principles pertaining to AI and cybersecurity.[429]

Another key point concerning future regulation would be the importance of multidisciplinarity. Risks in the cyber sphere associated with artificial intelligence cannot be tackled purely legally. Instead, there should be an interaction between specialists in law, technologies, policy-making, and ethics. Each discipline has its unique contribution to make – technologies give an idea of what artificial intelligence entails and what tools may be used to tackle its dangers, while law is about structure and implementation of these ideas into practice, while ethics makes sure human value system remains the focus of innovation.[430]

International cooperation is also expected to play an increasingly important role. Cyber threats are by nature global and cross-border in their effects. Thus, separate efforts made by different countries will not suffice to address these issues. Instead, it would be necessary to cooperate on many levels in order to tackle AI-powered cyber risks.

In the end, it becomes necessary to maintain the proper balance between the two. On the one side, an excess of regulations may prove detrimental to development. On the other hand, lack of regulation may lead to misuse and other harmful effects on the user's side. The balance will allow for both development to take place and safety from various dangers.

In summary, the evolution of the world of AI and cybersecurity will depend upon the ability of the legal framework to adjust to new circumstances. It is important to create adaptive and technology-neutral legislation, encourage accountability and cooperation among experts in multiple fields and even between countries. Thus, through achieving the proper balance, it will be possible to make the most out of the technology.[431]

---

[429] Supreme Court of India, Justice KS Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

[430] United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence (2021).

[431] NITI Aayog, National Strategy for Artificial Intelligence (2018).

Chapter 16
State and Sovereignty in Cyberspace: Government Frameworks, Laws, and Security Tools

Abu Toraab, Legal Researcher associated with the Uttar Pradesh Real Estate Regulatory Authority.

Abstract

The rapid expansion of cyberspace has fundamentally transformed the traditional concept of State sovereignty, extending its scope beyond territorial boundaries into the digital domain. This chapter examines the evolving notion of cyber sovereignty through a comprehensive analysis of constitutional principles, legislative frameworks, judicial interpretation, institutional mechanisms, and technological tools, with particular reference to India. It explores how the State seeks to assert regulatory authority over digital infrastructure, data flows, and online activities while simultaneously navigating the constraints imposed by fundamental rights and global interconnectedness.

The study critically analyses the constitutional foundations of cyber governance, focusing on the protection of freedom of speech and expression and the recognition of the right to privacy by the Supreme Court in landmark decisions such as Shreya Singhal v Union of India[432] and Justice KS Puttaswamy v Union of India[433] It further evaluates the legislative framework, including the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, highlighting their role in shaping India's cyber regulatory landscape. The chapter also examines the institutional architecture, including specialized agencies and policy frameworks, that supports cybersecurity governance. In addition, the analysis addresses the role of emerging technologies such as artificial intelligence, encryption, and data localization in strengthening State control, while also identifying the legal and ethical challenges associated with their use. The chapter situates India's approach within a broader global context, comparing different models of cyber governance and assessing the implications of divergent regulatory strategies.

The study concludes that cyber sovereignty is an evolving and contested concept that requires a balanced approach integrating legal, technological, and policy considerations. It emphasizes the need for adaptive regulatory frameworks, robust institutional mechanisms, and adherence to constitutional values in order to effectively govern cyberspace. The chapter contributes to the growing body of scholarship on digital governance by providing a nuanced understanding of the interplay between State authority, individual rights, and global norms in the digital age.

Keywords: *Cyber Sovereignty, Digital Governance, Right to Privacy, Information Technology Law, Data Protection*

---

[432] Shreya Singhal v Union of India (2015) 5 SCC 1 (SC).
[433] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC).

Introduction

The classical doctrine of sovereignty, deeply embedded in the evolution of modern nation-states, has historically been premised on territorial control, political authority, and the exclusive jurisdiction of States within defined geographical boundaries. This traditional conception, rooted in the Westphalian model, presupposes a clear demarcation between internal and external authority. However, the advent of cyberspace has profoundly disrupted this foundational understanding. In an increasingly interconnected digital ecosystem, where data flows transcend borders instantaneously, the State's ability to exercise control is both challenged and reconfigured.

Cyberspace is not merely a technological construct; it represents a dynamic socio-legal domain where individuals, corporations, and governments interact beyond the constraints of physical territory. The absence of tangible boundaries, coupled with the decentralized architecture of the internet, complicates the enforcement of domestic laws and the assertion of jurisdiction. Consequently, States have been compelled to reconceptualize sovereignty to address the realities of digital governance.

The notion of "cyber sovereignty" has emerged as a response to these challenges. It reflects the attempt of States to assert authority over digital infrastructure, regulate data flows, and maintain control over online activities within their jurisdiction. However, this assertion is neither absolute nor uncontested. It operates within a complex matrix of constitutional rights, international norms, and technological constraints.

This chapter undertakes a comprehensive examination of State sovereignty in cyberspace, with a particular focus on the Indian legal framework. It explores the constitutional underpinnings, statutory developments, judicial interpretations, and institutional mechanisms that collectively shape cyber governance. It further analyses the technological tools employed by States and the challenges inherent in balancing national security with individual freedoms. The discussion ultimately seeks to provide a nuanced understanding of cyber sovereignty as an evolving legal construct in the digital age.

Theoretical Evolution of Sovereignty in the Digital Era

The concept of sovereignty has undergone significant transformation in the digital age. Classical theorists such as Jean Bodin and Thomas Hobbes viewed sovereignty as the absolute authority of the State within its territorial boundaries, a notion reinforced by principles of international law like non-intervention and State equality.

However, cyberspace challenges this traditional framework. As a transnational domain, digital interactions often span multiple jurisdictions, complicating the enforcement of national laws and attribution of responsibility. This has given rise to competing models of cyber governance. One model supports a global and open internet with minimal State interference, while another—cyber sovereignty—emphasises the State's right to regulate digital spaces in line with domestic priorities.

India adopts a pragmatic, hybrid approach to cyber sovereignty. While supporting global connectivity, it increasingly asserts regulatory control to safeguard national interests, ensure data security, and uphold constitutional values. Measures such as data localisation, intermediary regulations, and strengthened cybersecurity frameworks reflect this balance between openness and control.

The rise of "data sovereignty" further underscores this shift. Data, often termed the "new oil," has become a vital economic and strategic asset. Consequently, States seek to ensure that data generated within their borders remains subject to their legal regimes.
At the same time, the growing influence of global digital platforms creates regulatory challenges. States must regulate these entities without stifling innovation or breaching international norms, requiring nuanced legal frameworks addressing competition, data protection, and content governance.

Judicial developments have also shaped the contours of digital sovereignty in India. In *Justice K.S. Puttaswamy v. Union of India*[434], the Supreme Court recognised privacy as a fundamental right, subjecting State action to tests of legality, necessity, and proportionality. Similarly, *Shreya Singhal v. Union of India*[435] affirmed the protection of online free speech. These decisions highlight that sovereignty in the digital era is constitutionally limited rather than absolute.

Internationally, cyber sovereignty remains underdeveloped. Although no binding global treaty exists, forums like the United Nations Group of Governmental Experts have articulated norms relating to State responsibility, non-intervention, and cooperation. However, the lack of uniform rules leads to regulatory fragmentation and jurisdictional conflicts.

Overall, sovereignty in the digital era is evolving from a purely territorial concept to one of networked governance. It requires States to adapt to decentralised and complex digital environments while balancing control with constitutional rights, innovation, and international cooperation.

Constitutional Foundations of Cyber Sovereignty in India

The Indian Constitution provides the normative framework for regulating cyberspace. Fundamental rights and directive principles collectively define the limits of State authority in the digital domain.
The right to freedom of speech and expression under Article 19(1)(a) extends to digital communication, including social media and online platforms. The Supreme Court in Shreya Singhal v Union of India held that restrictions on online speech must be narrowly tailored and consistent with constitutional guarantees.5 This decision underscores the importance of protecting digital expression while allowing reasonable regulation.
The right to privacy, recognised in Justice KS Puttaswamy v Union of India, constitutes a cornerstone of cyber governance.6 The Court affirmed that informational privacy is an essential aspect of personal liberty under Article 21. This principle has significant implications for data collection, surveillance, and AI-driven technologies.
Article 14, which guarantees equality before the law, also plays a crucial role in regulating algorithmic decision-making. AI systems, if not properly regulated, may perpetuate biases and lead to discriminatory outcomes. The constitutional mandate of equality requires that such systems be designed and implemented in a fair and non-arbitrary manner.

---

[434] Puttaswamy (n 3)
[435] Shreya Singhal (n 2)

Additionally, Article 300A protects property rights, which extend to digital assets and intellectual property. As data becomes a valuable economic resource, its regulation becomes central to the exercise of sovereignty.

Legislative Framework Governing Cyberspace

India's legislative framework for cyberspace has evolved considerably over the past two decades, with the Information Technology Act, 2000 forming its foundation. Initially enacted to provide legal recognition to electronic transactions, the Act has expanded into a key instrument of cyber governance, addressing offences related to cybercrime and digital regulation.

Over time, specific provisions of the Act have gained prominence. Section 69 empowers the government to intercept, monitor, and decrypt digital communications in the interest of national security, public order, and sovereignty. While this enhances the State's ability to respond to cyber threats, it also raises concerns regarding privacy and potential misuse. Similarly, Section 79 provides safe harbour protection to intermediaries, shielding them from liability for third-party content, subject to due diligence requirements. This provision reflects an effort to balance platform neutrality with accountability.

The regulatory landscape has been further shaped by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules impose obligations on intermediaries, including content moderation, grievance redressal, and the appointment of compliance officers. The introduction of traceability requirements for messaging platforms has sparked debate over the tension between encryption and law enforcement, signalling increased State oversight in line with cyber sovereignty.

A major recent development is the Digital Personal Data Protection Act, 2023, which establishes a comprehensive framework for personal data governance. It introduces concepts such as data fiduciaries and data principals, and emphasises consent-based processing, transparency, and data security. The Act represents a significant step towards aligning data regulation with constitutional principles.

Despite these advancements, challenges persist. Rapid technological developments—such as artificial intelligence, blockchain, and quantum computing—continue to outpace existing legal frameworks, creating regulatory gaps. Additionally, the transnational nature of cyberspace complicates enforcement and jurisdiction, highlighting the need for greater international cooperation.

Concerns also arise from the expansion of State powers in areas such as surveillance and content regulation. These must be carefully balanced against constitutional rights, particularly privacy and

freedom of expression. Judicial decisions like *Shreya Singhal v. Union of India*[436] and *Justice K.S. Puttaswamy v. Union of India*[437] have played a crucial role in maintaining this balance.

Overall, India's cyber law framework is dynamic and evolving. It combines statutory provisions, regulatory rules, and policy initiatives to address the complexities of digital governance. Moving forward, continuous adaptation will be essential to ensure security, foster innovation, and protect fundamental rights in the digital era.

Judicial Interpretation and Cyber Jurisprudence

The judiciary has played a crucial role in defining cyber sovereignty by balancing State authority with fundamental rights. Through its decisions, the Supreme Court has adapted constitutional principles to the digital context.

In *Anuradha Bhasin v. Union of India*[438], the Court recognised that access to the internet is integral to the exercise of fundamental rights and held that any restrictions must satisfy the test of proportionality and remain subject to judicial review. Similarly, in *Manohar Lal Sharma v. Union of India*[439], the Court addressed concerns of surveillance, emphasising that national security cannot justify unchecked violations of fundamental rights and must be accompanied by accountability.

Judicial engagement has also extended to intermediary liability and digital platform regulation. In *Facebook Inc. v. Union of India*, the Court examined traceability requirements on encrypted platforms like WhatsApp, highlighting the tension between privacy and law enforcement. The case illustrates the broader challenge of balancing technological design with legal and constitutional safeguards.

The judiciary has further acknowledged the internet as an essential component of modern life, linking it to rights such as education, trade, and democratic participation. This recognition elevates digital access to a matter of constitutional significance and influences policy and regulatory approaches.

However, cyber jurisprudence has its limitations. Judicial intervention is often reactive, addressing issues only after disputes arise. Additionally, the technical complexity of digital technologies can pose challenges for courts, underscoring the need for specialised expertise.

Despite these constraints, the judiciary remains central to the evolution of cyber law in India. Its decisions establish guiding principles that protect individual rights while enabling the State to regulate cyberspace. As digital technologies continue to evolve, judicial interpretation will remain vital in shaping a balanced and rights-oriented framework for digital governance.

Government Frameworks and Institutional Mechanisms

India's cybersecurity framework is built around key institutions such as the Indian Computer Emergency Response Team (CERT-In), which acts as the national nodal agency for responding to cyber incidents, issuing advisories, and coordinating with stakeholders. Alongside it, the National Critical Information Infrastructure Protection Centre (NCIIPC) focuses on protecting critical sectors like

---

[436] Shreya Singhal (n 2)

[437] Puttaswamy (n 3)

[438] Anuradha Bhasin v Union of India (2020) 3 SCC 637.

[439] Manohar Lal Sharma v Union of India (2021 SCC Online SC 985).

energy, banking, and telecommunications. These institutions reflect the recognition that cyber threats are not only technical issues but also matters of national security and economic stability.

The broader policy framework is guided by the National Cyber Security Policy, which aims to build a secure and resilient cyberspace through capacity building, awareness, and public-private partnerships. Regulatory control has expanded through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose obligations on digital platforms such as content moderation, grievance redressal, and cooperation with law enforcement. This marks a shift towards greater State oversight and accountability in line with cyber sovereignty.

Sectoral regulators such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) further strengthen cybersecurity within their respective domains by issuing guidelines and resilience frameworks. In addition, specialised cybercrime cells, growing use of cyber forensics, and initiatives for skill development and research contribute to improving enforcement and institutional capacity.

Despite this comprehensive framework, challenges remain, including coordination gaps among agencies, rapid technological changes, and concerns about transparency and accountability in the exercise of State power. Judicial oversight plays a key role in addressing these concerns by ensuring that cybersecurity measures operate within constitutional limits. Overall, India's institutional framework is evolving, and its effectiveness will depend on adaptability, coordination, and respect for fundamental rights.

Security Tools and Technological Measures

Cyber governance today relies heavily on technological tools that operationalise legal and policy frameworks. In India, these measures include surveillance systems, encryption technologies, artificial intelligence, and network security tools. Surveillance, enabled under statutory provisions like Section 69 of the Information Technology Act, 2000, allows the State to monitor digital communications for national security and law enforcement. While such systems are essential for preventing cyber threats, they raise concerns about privacy and require safeguards in line with the principles laid down in *Justice K.S. Puttaswamy v. Union of India*[440]. Lawful interception mechanisms further enable regulated access to communications, but their legitimacy depends on procedural oversight and accountability.

Encryption is another key component, ensuring the confidentiality and integrity of data across platforms such as banking and messaging services. However, strong encryption creates challenges for law enforcement, leading to debates over traceability and regulation. Similarly, emerging technologies like artificial intelligence and machine learning are increasingly used to detect threats, analyse patterns, and predict cyberattacks. While these tools enhance efficiency and enable proactive responses, they also raise issues of transparency, accountability, and potential bias.

Additional measures include data localisation policies, which seek to enhance State control over data by requiring storage within national boundaries, and network security tools such as firewalls and

[440] Puttaswamy (n 3)

intrusion detection systems that protect digital infrastructure. Digital forensics has also become crucial for investigating cyber offences, supported by the legal recognition of electronic evidence under Section 65B of the Indian Evidence Act, 1872. Technologies like blockchain and practices such as vulnerability assessment and penetration testing further strengthen cybersecurity by improving data integrity and identifying system weaknesses.

Despite these advancements, challenges remain in terms of coordination, implementation, and the rapid evolution of technology. The use of such tools also raises legal and ethical concerns, particularly regarding privacy, surveillance, and regulatory overreach. Therefore, while technological measures are central to cyber governance and the assertion of State sovereignty, their deployment must be balanced with constitutional safeguards, transparency, and adherence to the rule of law.

Challenges to Cyber Sovereignty

The assertion of cyber sovereignty faces inherent challenges due to the borderless and transnational nature of cyberspace. Digital communications and data flows frequently cross multiple jurisdictions, making it difficult to identify applicable laws and enforce them effectively. This results in jurisdictional ambiguities, particularly in cases involving cybercrime, data breaches, and cross-border transactions. The lack of a comprehensive international legal framework further contributes to fragmented and sometimes conflicting regulatory approaches.

Another significant challenge arises from the dominance of multinational technology companies. Global digital platforms operate across borders and control vast amounts of data and communication infrastructure, often limiting the ability of States to exercise effective regulatory control. Measures such as data localisation and intermediary regulations attempt to address this imbalance but may also create friction between national interests and the global nature of digital markets.

Balancing national security with the protection of fundamental rights remains a critical concern. States increasingly rely on surveillance, data access, and content regulation to maintain security and public order. However, excessive or unchecked use of these powers can undermine privacy and freedom of expression. Judicial decisions such as *Justice K.S. Puttaswamy v. Union of India* and *Shreya Singhal v. Union of India* emphasise the need for safeguards, proportionality, and accountability in such measures.

Rapid technological advancements present another major obstacle. Technologies such as artificial intelligence, blockchain, and quantum computing evolve faster than legal frameworks, creating regulatory gaps and uncertainties. These developments introduce complex issues relating to accountability, liability, and governance, requiring continuous legal adaptation and innovation.

Data governance further complicates the exercise of cyber sovereignty. As data becomes a key economic and strategic resource, States seek greater control through measures like data localisation. While such policies enhance regulatory oversight and security, they may also increase compliance costs, disrupt global trade, and contribute to the fragmentation of the internet.

Finally, institutional and international limitations hinder effective cyber governance. The enforcement of cyber laws requires specialised expertise, robust infrastructure, and coordination among multiple agencies, which can be challenging to achieve. Additionally, cyber threats often originate beyond national borders, making attribution and response difficult. Addressing these issues requires stronger institutional capacity, improved coordination, and greater international cooperation, while ensuring adherence to constitutional principles.

Global Perspectives

The governance of cyberspace cannot be understood in isolation, as it operates within a highly interconnected global environment. Since digital activities transcend national borders, actions in one jurisdiction often affect others. As a result, States have adopted diverse approaches to cyber governance based on their political systems, economic priorities, and security concerns. These differing approaches collectively shape the evolving global discourse on cyber sovereignty.[441]

Broadly, three dominant models of cyber governance can be identified: the open internet model, the regulated sovereignty model, and the state-centric model. The open internet model, associated with countries such as the United States, emphasises the free flow of information, minimal State intervention, and protection of individual liberties. While it promotes innovation and global connectivity, concerns relating to misinformation, cybercrime, and national security have led to increased regulatory scrutiny even within this model.[442]

The regulated sovereignty model, exemplified by the European Union, seeks to balance openness with strong legal oversight. Instruments such as the General Data Protection Regulation (GDPR) establish stringent standards for data protection and privacy, granting individuals greater control over their personal data.[443] This framework has had a global influence, shaping data protection regimes in several jurisdictions, including India.

In contrast, the state-centric model, followed by countries such as China and Russia, emphasises extensive State control over digital infrastructure, data flows, and online content. Measures such as internet filtering, surveillance, and data localisation are used to maintain national security and political stability. However, this model has been widely criticised for restricting freedom of expression and limiting access to information.[444]

India adopts a hybrid approach, combining elements of openness with regulatory control. While supporting a free and accessible internet to promote innovation and economic growth, India has strengthened its regulatory framework through data protection laws, intermediary regulations, and

---

[441] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006).
[442] Milton L Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010).
[443] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L 119/1.
[444] Ronald J Deibert, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi Press 2020).

cybersecurity measures. This approach reflects an attempt to balance domestic priorities with participation in the global digital economy.[445]

At the international level, cyber governance remains fragmented due to the absence of a binding global framework. Initiatives such as the United Nations Group of Governmental Experts and the Open-Ended Working Group have developed non-binding norms on responsible State behaviour, including principles of sovereignty and non-intervention.[446] However, differences in national interests continue to hinder consensus, raising the risk of a "splinternet" and underscoring the need for greater international cooperation and harmonisation.

Conclusion

The transformation of cyberspace into a critical domain of governance has fundamentally altered the traditional understanding of State sovereignty. No longer confined to territorial boundaries, sovereignty in the digital age extends into networks, data infrastructures, and virtual interactions that transcend geographical limits. This evolution has compelled States, including India, to reimagine their regulatory frameworks and institutional mechanisms in order to effectively govern an increasingly complex and interconnected digital environment.

This chapter has examined the multifaceted dimensions of cyber sovereignty through constitutional, legislative, judicial, institutional, and technological lenses. At the constitutional level, the Indian framework establishes a delicate balance between State authority and individual rights. The recognition of freedom of speech and expression in the digital sphere, as affirmed in Shreya Singhal v Union of India, and the articulation of privacy as a fundamental right in Justice KS Puttaswamy v Union of India16, underscore the centrality of constitutional values in shaping cyber governance. These decisions ensure that the expansion of State power in cyberspace is subject to the principles of legality, necessity, and proportionality.

From a legislative perspective, instruments such as the Information Technology Act, 200017 and the Digital Personal Data Protection Act, 2023[447] provide the statutory foundation for regulating digital activities. These laws, supplemented by subordinate legislation and policy frameworks, reflect an evolving attempt to address issues ranging from cybercrime and intermediary liability to data protection and cybersecurity. However, the rapid pace of technological change continues to challenge the adequacy of existing legal frameworks, necessitating continuous reform and adaptation.

Judicial interpretation has played a pivotal role in bridging the gap between law and technology. Through its jurisprudence, the Supreme Court has not only protected fundamental rights but also shaped the contours of cyber regulation in India. Decisions relating to internet access, surveillance, and intermediary liability illustrate the judiciary's role as a guardian of constitutional principles in the digital domain.

---

[445] Anirudh Burman, 'Cyber Sovereignty and India's Digital Policy' (Carnegie India, 2021).

[446] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2013, 2015, 2021); UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (2021).

[447] Digital Personal Data Protection Act 2023

The institutional architecture supporting cyber governance further reinforces the State's capacity to assert sovereignty. Agencies responsible for cybersecurity, critical infrastructure protection, and law enforcement operate within a coordinated framework designed to respond to emerging threats. At the same time, the deployment of technological tools—such as surveillance systems, encryption mechanisms, and artificial intelligence—has enhanced the operational capabilities of the State. These tools, however, must be employed with caution, ensuring that their use does not undermine the very rights they are intended to protect.

The challenges to cyber sovereignty remain substantial. Jurisdictional complexities, the dominance of multinational technology companies, the tension between security and privacy, and the risk of internet fragmentation all pose significant obstacles. These challenges are compounded by the absence of a comprehensive international legal framework, leading to divergent approaches and potential conflicts among States.

In this context, global perspectives provide valuable insights into alternative models of governance. While some jurisdictions emphasise openness and innovation, others prioritise control and security. India's approach, characterised by a balance between regulation and openness, reflects its unique constitutional and socio-economic context. The ability to maintain this balance will be crucial in ensuring that cyber sovereignty is exercised in a manner that promotes both national interests and global cooperation.

Ultimately, the future of cyber sovereignty lies in the development of a holistic and adaptive framework that integrates legal, technological, and policy considerations. Such a framework must be grounded in constitutional values, responsive to technological advancements, and aligned with international norms. It must also recognise the importance of collabouration among States, private actors, and civil society in addressing the challenges of cyberspace.

As the digital landscape continues to evolve, the concept of sovereignty will remain dynamic, requiring continuous re-evaluation and innovation. The task before policymakers, jurists, and scholars is not merely to regulate cyberspace but to shape it in a manner that upholds the rule of law, protects individual rights, and fosters a secure and inclusive digital future.

Chapter - 17

Anticipating Tomorrow's Threats: Strategic Foresight in Cybersecurity

Dr. Chandrima Chakraborty, Assistant Professor, School Of Legal Studies, Swami Vivekananda University and Ankita Mukherjee, Assistant Professor, School of Legal Studies, Swami Vivekananda University.

Abstract

In an increasingly interconnected digital landscape, cybersecurity is no longer a reactive discipline but a strategic imperative that demands anticipation and adaptability. This paper explores the role of strategic foresight in identifying and mitigating emerging cyber threats before they materialize into large-scale disruptions. By integrating methodologies such as horizon scanning, scenario planning, and trend analysis, organizations can move beyond traditional defense mechanisms and adopt a proactive security posture.

The study highlights how evolving technologies—including artificial intelligence, quantum computing, and the Internet of Things—are reshaping the threat landscape, introducing complex vulnerabilities alongside unprecedented opportunities. Cyber adversaries are leveraging automation, deepfakes, and sophisticated attack vectors, necessitating a forward-looking approach that accounts for uncertainty and rapid technological change. Strategic foresight enables decision-makers to envision multiple plausible futures, assess potential risks, and design resilient systems capable of withstanding unforeseen challenges.

Furthermore, the paper emphasizes the importance of cross-sector collabouration, intelligence sharing, and policy alignment in strengthening global cybersecurity readiness. It examines case studies where foresight-driven strategies have enhanced threat detection, improved incident response, and reduced organizational risk exposure. The integration of foresight into cybersecurity governance frameworks is presented as a critical factor in achieving long-term digital resilience.

Ultimately, this research argues that anticipating tomorrow's cyber threats requires a shift in mindset—from short-term risk management to continuous, future-oriented planning. Organizations that embed strategic foresight into their cybersecurity practices will be better equipped to navigate uncertainty, safeguard critical assets, and maintain trust in an increasingly volatile digital environment.

Keywords: *Strategic Foresight, Cyber Threat Intelligence, Emerging Technologies, Proactive Cybersecurity, Digital Resilience*

Introduction

Cybersecurity is often compared with arms race. Every new defence act as an inspiration for a new attack. Every patch tries to uncovers some vulnerability. Yet, in the persistent myopia, the organisation often overlooks a crucial truth: the most dangerous cyber threats are not the ones we see today, but the ones silently shaping beneath the surface. Strategic anticipation in cybersecurity is therefore not merely an academic idea; it is an indispensable requirement for governments, businesses, and societies that depend on digital configuration.

In classrooms, boardrooms, and policy discussions, cybersecurity is still too frequently treated as a technical problem in lieu of strategic one. Firewalls are installed, antivirus software is updated, and compliance checklists are completed. But adversaries are not. They innovate, cooperate, and adapt. Criminal groups use artificial intelligence, whereas state actors' experiment with quantum technologies, and hacktivists mobilise through social platforms. A purely passive approach cannot keep pace. Strategic foresight assists organisations envisage possible futures, identify emerging threats, and prepare before crises materialise.

This chapter demonstrate how strategic foresight can modify cybersecurity from reactive defence into proactive resilience. It scrutinises the changing threat landscape, methods of foresight, empirical implementation strategies, ethical challenges, and the role of education and governance. The objective is to humanise cybersecurity by exhibiting that behind every attack are persons, institutions, and choices—and foresight allow us to shape better outcomes.

Understanding the Changing Cyber Threat Landscape

Cyber threats have evolved from isolated acts of curiosity into complex universal operations. In the formative years of computing, hackers frequently sought reputation or intellectual challenge. Today, cybercrime is a multi-billion-dollar industry. Ransomware gangs run like big agencies, with customer service teams and profit-sharing models. Nation-states manage cyber espionage to influence elections, steal intellectual property, and disrupt infrastructure. Terrorist groups traverse digital sabotage. Even standard users unknowingly participate through botnets or data leaks.[448]

Several trends define today's threat landscape:

First, automation has accelerated attacks. Malware can now scan millions of devices in seconds. Artificial intelligence permits attackers to spawn realistic phishing emails, deep-fake voices, and 'automated vulnerability discovery tools'.[449]

Second, interconnectivity has enlarged risk. Smart homes, wearable devices, industrial control systems, and cloud computing create new gateways. A vulnerability in a small supplier can compromise a complete supply chain.

---

[448] Bruce Schneier, 'Click Here to Kill Everybody: Security and Survival in a Hyper-connected World', WW Norton 2018.
[449] Ibid

Third, geopolitical tensions progressively play out in cyberspace. Critical infrastructure such as power grids, hospitals, and financial networks has become targets during international disputes.

Fourth, data has become the new currency. Personal information, trade secrets, and biometric identifiers are valuable assets. Once stolen, they cannot easily be restored.

These changes portrays that cybersecurity is no longer about protecting computers only. It is about safeguarding trust in digital society.

What is Strategic Foresight?

Strategic foresight is a disciplined approach to thinking about the time ahead. It does not endeavour to predict exactly the future. Instead, it reconnoitres multiple plausible futures to assist decision-makers prepare. In cybersecurity, foresight means asking questions such as: What new technologies might generate vulnerabilities? How criminal groups might evolve? What social trends could enlarge exposure to digital harm?

Foresight differs from conventional hazards assessment in three ways. First, it considers beyond known threats. Second, it emphasises enduring thinking. Third, it amalgamates technological, political, economic, and social factors. A new encryption method, for instance, may affect privacy law, international relations, and consumer trust simultaneously.[450]

Common foresight tools include 'scenario planning, horizon scanning, trend analysis, Delphi surveys, and red teaming exercises.'[451] Each method encourages organisations to envisage alternative futures and test their preparedness.

Why Strategic Foresight Matters in Cybersecurity

Cybersecurity failures often appear from surprise. Organisations focus largely on present risks while neglecting growing ones. Strategic foresight reduces surprise by increasing awareness.

One benefit is resilience. When businesses anticipate interruptions, they may create flexible systems that adjust quickly. For example, preparing for supply chain assaults may encourage vendor variety and the use of strong monitoring technologies.

Another advantage is improved policy. Governments that forecast cyber dangers might create legislation to encourage safe software development, responsible data exchange, and critical infrastructure security.

Foresight is also useful in enhancing schooling. Universities can aim to integrate cybersecurity jobs, rather than outmoded technology, in future curriculum teaching capabilities.

Finally, foresight builds trust. When citizens notices institutions prepared for cyber crises, confidence in digital systems increases.[452]

---

[450] Paul Cornish and others, 'On Cyber Warfare', Chatham House Report 2010.
[451] Ibid.
[452] Joseph Nye Jr, 'Deterrence and Dissuasion in Cyberspace' (2017) 41 International Security 44.

Methods of Strategic Foresight in Cybersecurity

- **Horizon Scanning**

Horizon scanning recognises weak signals. Analysts monitor technological developments, academic research, social trends, and criminal activity. For example, early research into quantum computing divulges the possibility that future machines could shatter current encryption. Organisations that identified this risk began developing post-quantum cryptography.

- **Scenario Planning**

Scenario planning envisages detailed future worlds. A cybersecurity team might traverse scenarios such as 'global internet fragmentation, widespread AI-driven cybercrime, or collapse of trust in digital identity systems.' These scenarios help organisations test strategies under various conditions.

- **Red Teaming and War Gaming**

Red teaming entails conducting simulated assaults to uncover weaknesses. War gaming takes this concept to a strategic level, investigating how enemies may use political or economic factors. These exercises reveal blind spots and encourage creative thinking.

- **Technology Forecasting**

Technology forecasting examines emerging innovations such as artificial intelligence, biotechnology, and quantum computing. Each new technology generates opportunities and risks. Forecasting assists organisations prepare for both.

- **Stakeholder Engagement**

Cybersecurity is not just technical. Lawyers, sociologists, economists, psychologists, and educators all influence outcomes. Foresight exercises involving manifold stakeholders produce more realistic insights.[453]

- **Implementing Strategic Foresight in Organisations**

Strategic foresight should not endure an isolated workshop. It must flatter parts of organisational culture.

First, leadership commitment is essential. Executives must allot resources for foresight research and merge results into planning. Without leadership, foresight becomes symbolic rather than practical.

Second, interdisciplinary squad are necessary. Cybersecurity professionals should collabourate with specialist in public policy, and behavioural science. Human error remains a major reason of breaches, so understanding psychology matters.

Third, continuous learning is pivotal. Cyber threats develop quickly, therefore foresight must be ongoing. Scenarios, threat models, and training courses are regularly updated to ensure their relevance.

---

[453] Joseph Nye Jr, 'Deterrence and Dissuasion in Cyberspace' (2017) 41 International Security 44.

Fourth, communication is vital. Technical specialists must translate prescient judgement into understandable terms for decision-makers. Storytelling may make abstract dangers seem more logical. Fifth, coordination between organisations strengthens security. Sharing threat intelligence across businesses and nations reduces redundancy and improves readiness.[454]

Ethical Challenges in Cybersecurity Foresight

Apprehending menace promote ethical questions. Surveillance system stewardship can threaten privacy. Predictive algorithms could conserve prejudice. Governments may substantiate surveillance in the name of national security.

Strategic foresight must therefore integrate 'holistic ethical analysis'. Decisions about 'data collection, artificial intelligence, and digital governance' should contemplate human rights. 'Transparency and accountability' boost legitimacy.[240]

Another challenge is inequality. Affluent institutions can fund next generation defense, while small businesses and public institutions suffer. Foresight shall eliminate the ambiguities by advocating for accessible, secure technology and training.

Strategic Foresight and Public Policy

Governments contribute a critical role in advancing the cyber security paradigm. 'National strategies, international agreements, and legislative frameworks' influence behaviour. Public policy can foster sturdy software development, demand breach disclosure, and protect critical infrastructure. It can also advance pioneering research such as 'quantum-resistant encryption'.

The Human Dimension of Cybersecurity

Behind every 'cyber breach' lies a personal story. Interacting with a malicious URL because they are tired. A student tends to downloading unauthorized software because it is affordable. A criminal group recruits emerging tech talent from marginalised communities. Strategic foresight must therefore combat social conditions that create vulnerability. Awareness campaigns, ethical technology design, and inclusive digital policies mitigate risk. When systems are user-friendly and transparent, people choose other options which are secure. When education is accessible, less people turn to cybercrime.[455]

Education policy matters are important concern. Schools and universities should educate on' digital literacy, ethical hacking, and critical thinking'. A society that recognises cybersecurity is more resilient.

---

[454] Herbert Lin, 'Cyber Conflict and International Humanitarian Law' (2012) 89 International Review of the Red Cross 515.
[240] Ibid.
[455] Michel Godet, 'Creating Futures: Scenario Planning as a Strategic Management Tool', Economica 2001.

Future Threats to Watch

Several emerging trends may shape cybersecurity in coming decades:

- Quantum computing could decipher existing cryptanalysis.
- Artificial intelligence may automatize cyberattacks and generate persuade misinformation.
- Biometric systems could be misused, creating Synthetic Identity Theft.
- Space-based infrastructure such as satellites may eventually become cyber targets.
- Internet-of-Things devices could allow large-scale disruption of cities.[456]

Strategic foresight helps various organisations systematize for these possibilities without panic. It spurs strategic thinking instead of crisis-driven reaction.

Looking ahead, cybersecurity experts must focus to an array of next-generation technologies and social trends that are likely to metamorphosis of digital vulnerabilities. These are not faint possibilities; many are already surreptitiously developing, and their ramifications may be intense if left unprepared for.

One of the most important future risks is 'quantum computing'. When practical, extensive quantum machines arrive, they may shatter widely used 'encryption systems' that protect banking, 'government communication', and personal data. This does not mean security will fall apart overnight, but organisations that causes hindrance in transitioning to quantum-resistant cryptography could face sudden exposure. Planning for this transition now is important because cryptographic change takes years.

Artificial intelligence represents a second wave of transformation. While AI tools reinforce defence through automatic detection and quick response, they also authorize the attackers. 'Deep fake audio and video' can be used for 'fraud, political manipulation, or corporate espionage'. AI-generated phishing emails are increasingly imperceptible as they imitate human writing techniques and local languages. In the future, malware might evolve on its own, learning from failed attacks and upgrade automatically.

A third concern lies in biometric security. 'Fingerprints, facial recognition, and voice identification' are incrementally used for authentication. Unlike 'passwords, biometric data' cannot be modified once stolen. If huge biometric databases are breached, individuals are likely to endure prolonged disruption of identity risks. Strategic foresight therefore demands combining biometric systems with enhanced 'confidentiality safeguards and backup verification methods'.

The sudden expansion of the 'Internet of Things'[243] is another critical area. 'Smart homes, connected cars, medical implants, and industrial sensors'[244] generate convenience but also widen the attack surface. Weak security in one device can enable the hackers to enter larger networks. Future cyber breaches may target complete cities by disrupting the whole network of the satellite systems, water treatment plants, or big payment systems of any institutes. Securing web and devices is therefore a

---

[456] Michel Godet, 'Creating Futures: Scenario Planning as a Strategic Management Tool', Economica 2001
[243] Lawrence Freedman, 'Strategy: A History', Oxford University Press 2013. [244] Ibid.

concern of public safety, not merely a consumer choice. Space infrastructure is also venturing within cybersecurity planning. Satellites negotiate with communication, navigation, and weather forecasting. As more countries and private corporation launch satellites, the risk of cyber interference enhances. A synchronised attack on satellite systems could obstruct banking transactions, aviation routes, and emergency services co-occurrent.

Finally, social and psychological threats must be taken into account. 'Disinformation campaigns, online radicalisation, and data-driven political manipulation'[457] can lead to democratic backsliding without a single line of malicious code. Cybersecurity foresight must therefore embrace media literacy, ethical platform design, and strong legal frameworks.

None of these threats should amplify terror or technological pessimism. Instead, they remind us that cybersecurity is an unwavering allegiance. By identifying risks at an initial phase, investing in research, giving importance to education, and encouraging various organisations across sectors, societies can meet future challenges with utmost confidence rather than crisis or fear.

Creating a foresight-driven organisation requires patience. Employees must feel inspired to think creatively and further be open to ask question in various assumptions. Training programmes should include simulation drills and interdisciplinary dialogue. Organisations should focus on long-term thinking rather than short-term fixes.

Conclusion

In an era of an increasing ttechnological modernization, *Anticipating Tomorrow's Threats: Strategic Foresight in Cybersecurity* postulates a major truth: the future of cybersecurity cannot be affixed by counteractive measures alone. As advanced technologies such as 'artificial intelligence, quantum computing, sovereign systems, and hyperconnected infrastructures' reshape the international landscape, the threat environment advances in equidistant, comparatively faster than conventional defense mechanisms can adapt. Strategic foresight therefore appears not as an opulence, but as an essential requirement for organizations and nations looking for continued digital resilience.

The chapter emphasizes that anticipating tomorrow's threats entails more than technical proficiency or advanced security tools. Cybersecurity is not only a technical discipline; it is a social, political, and ethical challenge shaped by human decisions, power structures, and global inequalities. Every vulnerability outlines alternatives in system design, governance, and human behavior. Strategic foresight dispenses a structured way to envision possible futures, prophesy emerging risks, and prepare responsibly for uncertainty. It calls for the integration of technological expertise with fascination, empathy, and ethical reflection.

Through 'horizon scanning, scenario planning, and predictive analytics', executives can identify weak signals before they escalate into cataclysmic upheaval. By inserting foresight into organizational culture, institutions shift from a reactive posture of troubleshooting to a proactive stance of preparedness and adaptability. This kind of new initiatives encourages investment in resilient architectures, flexible policies, and professional development capable of responding to rapidly

[457] Herbert Lin, 'Cyber Conflict and International Humanitarian Law' (2012) 89 International Review of the Red Cross 515.

changing threats. Collabouration is midway to this approach. Governments, private enterprises, academia, and civil society must share intelligence and coordinate strategies to mitigate risk that transcend borders and sectors. Collective learning, transparent communication, and shared responsibility strengthen global cybersecurity ecosystems and reduce the likelihood of strategic startle.

Ultimately, the chapter delivers a simple but compelling message: the fate of cybersecurity is not predetermined. Strategic foresight repudiates to prognosticate the future with certainty; rather, it equips communities to anticipating probable developments with confidence and purpose. Through ‘deliberate planning, ethical awareness, and cooperative action’, we can convert ‘uncertainty into opportunity and construct resilient technological futures’. In doing so, strategic foresight becomes the cornerstone of ‘sustainable cybersecurity’—ensuring that tomorrow’s cyberspace is not merely defended, but circumspectly and responsibly shaped.

----------**********----------

Chapter 18

Cyber Vulnerabilities of Informal Workers in India

Antu Rani Majumdar, Assistant Professor, Swami Vivekananda University, Dr. Malay Adhikari, Assistant Professor, Amity University, Kolkata and Prof. (Dr.) Pradeepta Kishore Sahoo, Principal, Law College Durgapur.

Abstract

The rapid digitalisation of labour markets has transformed the nature of work, extending technological systems into informal and contract-based employment. While these developments promise efficiency, transparency, and inclusion, they simultaneously expose workers to emerging cyber vulnerabilities. This chapter examines the paradox of informal workers in the digital age, where informal and contract workers become increasingly visible through data collection yet remain legally unprotected. It argues that cyber risks such as data exploitation, identity theft, algorithmic wage manipulation, workplace surveillance, and online harassment are structurally embedded within contemporary labour arrangements.

Adopting a socio-legal approach, the chapter critically analyses the limitations of existing legal frameworks, including the Code on Social Security, 2020, the Code on Occupational Safety, Health and Working Conditions, 2020, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, highlighting their fragmented and inadequate response to worker-centric cyber harms. It further explores how power imbalances, digital illiteracy, and the absence of accountability in contract labour arrangements exacerbate these vulnerabilities.

The chapter contends that cybersecurity must be reconceptualised as a labour rights issue rather than merely a technological concern. It calls for an integrated regulatory framework that recognises digital safety as part of working conditions, ensures employer accountability, and protects the informational privacy and dignity of workers. By bridging the gap between cyber law and labour law, this study contributes to the evolving discourse on digital labour governance in India.

Keywords: *Informal Labour, Cyber Vulnerability, Data Protection and Algorithmic Control*

1. Introduction

The changes witnessed in labour markets over the last decades have been strongly influenced by the growth of gig economy and contract labour. Technology has changed the way people participate in labour markets as labourers have an opportunity to engage in flexible employment and perform their tasks under contracts without necessarily being formally employed. Although this change has presented economic gains, it has also deprived the participants of some benefits that would be available in case of permanent employment. The main issue with contract labour and informality in labour markets is that neither of these categories enjoys a number of benefits, such as health insurance, leaves,

job stability, and protection under labour laws. Participation of informal labour in economic activity is crucial; however, it goes unnoticed, which is why this type of labour is labelled "informal."[458]

Invisibility in this case not only refers to the economic marginalization of such people, but also involves invisibility in the cyberspace domain. Given that such people have to rely on digital technology to secure jobs and perform tasks, cybersecurity becomes a significant concern for them. Irrespective of the role one plays, be it a cab driver who needs to seek customers through online platforms, a person who arranges deliveries using apps, a freelancer who finds clients through websites, or a domestic helper who seeks jobs online, digital technology becomes a crucial platform for earning a livelihood.[459] But at the same time, the need to use digital technology opens the door to several cybersecurity issues. In the absence of any knowledge about digital technology and without any assistance from any institution, such people become highly susceptible to phishing, scams, identity theft, and other forms of cybercrime.

Moreover, the workplace in the platform system can involve gathering and analyzing large amounts of data about workers' behaviour and personal information. The degree of control by the informal workers over the collected data, its management, and accessibility is minimal. The algorithm behind the task allocation, the evaluation of workers' performance, and wage determination is very obscure and makes the workers vulnerable to exploitation, monitoring, and even blocking of their accounts. It follows that cybersecurity cannot be regarded as only a technical problem.

Considering the above discussion, therefore, it is apparent that a dire need for action exists. It is necessary to formulate measures that ensure that the digitalization era takes into consideration the protection of informal workers. Ensuring that informal workers have their cyberspace protected is necessary to ensure the protection of worker rights via measures that ensure that this is accomplished. This will ensure that digitalization does not result in even greater inequalities but instead promotes the objectives of inclusiveness.

2. Understanding informal worker

The informal labour force, therefore, can be defined as those kinds of labour that are essential in the process of producing goods and services in the economy, yet they lack any official acknowledgment in the system of recognition. The term 'informal labour' refers to that kind of labour force which lacks both recognition and appreciation from any official policy or law formulated by the government.[460]

---

[458] VV Giri National Labour Institute, *Gig and Platform Workers: Vision Towards Social Protection in India* (VVGNLI 2021).

[459] National Commission for Enterprises in the Unorganised Sector (NCEUS), *Report on Conditions of Work and Promotion of Livelihoods in the Unorganised Sector* (Government of India 2007).

[460] Kunal Sen and Ravi Kanbur, 'Informality in India: Causes, Consequences and Policy Responses' (2015) *Indian Journal of Labour Economics*.

This is because informal labour includes those kinds of productive labourers like domestic labourers, street vendors, homeworkers, etc.

In addition, another aspect that contributes to informal employment is the lack of an employment agreement outlining terms of employment. Without evidence backing their allegations, the employers can alter payment rates, number of working hours, and duties allocated to the worker at will with no fear of any repercussions whatsoever. In this respect, informal employment shields the employer or his agent from any possible consequences of their actions. One of the problems encountered by workers engaging in informal employment is the issue of job insecurity. The workers have no guarantee they will be able to secure similar jobs in the coming day. They are engaged on either a daily basis or based on piece work. Conversely, during formal employment, individuals are able to access various social security services including medical services and compensation for injuries. Carefulness is going to be vital when it comes to planning, since if such people have an accident or get ill, they will be well prepared to deal with it. This implies that it would be difficult for them to plan their future life as a result of the unpredictability of the economy.

Informal workplace conditions may also be as a result of lack of protection. Many laws relating to work are written in the assumption that formal employment has occurred. Informal workers thus are not covered by law since they do not work within its realm. Even if there exist laws that cover informal employees, it remains difficult for such people to use the laws since they are rarely implemented.

However, in the case of the employee group under discussion, the application of the technology involves only consumption of information and not participating in the process. They have no knowledge regarding the techniques of negotiations related to the use of the digital technology and the power dynamics that exist in negotiating the use of the digital technology at their workplace. The process of negotiation is even more difficult for them because there are no organizations like trade unions to fight their cause.[461]

3. Digitalization and the Informal Workforce

Indeed, technology has brought about various implications on the labour market, particularly for people who depend on the informal economy for their living. Due to the presence of technology inventions like mobile phones, mobile money transfers, software programs, and identity verification systems, people have been able to get jobs and make some money. It is important to point out that the shift in power relations within the labour market has been facilitated by these developments.

3.1. Platform-Based Work and Algorithmic Control

There is no doubt that gig labour should be mentioned as an example of the effects of digitalization. The intermediary role of the platforms will consist in bringing together people who want to perform

[461] Internet Freedom Foundation, *Privacy and Data Protection in India: Issues and Challenges* (IFF Report).

tasks and people who require these tasks to be performed.[462] Generally, the people providing their services will be regarded as independent contractors and not their employees.

This kind of work would surely be extremely easy to perform, considering the factor of digitization. However, aside from the advantage mentioned above, some problems arise when it comes to digitization in relation to this type of work. This is due to the fact that the processes involved, such as task assignment, assessment, and remuneration for the effort expended, have become automatic. In addition, individuals performing this kind of digitized task do not truly understand how it operates. Furthermore, there is always the possibility of blocking the user account.

3.2. Digital Payments and Financial Exposure

There have been numerous changes in the life of informal employees due to the adoption of digital money transaction systems. It is because of the existence of digital wallets as well as other forms of digital money transaction services like fast money and online banking that make it possible for informal workers to act without necessarily carrying any cash. Digital money transaction systems not only facilitate access to money for informal employees but also makes it possible for them to engage in financial transactions.

Nonetheless, although it is true that there arise some benefits from this transition, some challenges associated with this very transition revolve around exposing the informal labour force to different forms of danger. Indeed, since the informal labourers get their money using the technological method, they open themselves up to different dangers, especially hacking.[463]

3.3. Online Identity Systems and Data Dependence

Moreover, the mandatory use of digital IDs for accessing services not only at the office but also at government departments has also brought the informal workers into the digital age. It is important to have IDs, biometrics, and accounts on mobile devices to access the digital platform.

On the contrary, while these tools may have been quite useful in ensuring that verifying information and reducing paperwork was easy, the reality is that they end up being tools for gathering data on people. The people working in the informal economy do not know how their data is being managed. [464] Dependence on digital identity can therefore become a double-edged sword facilitating access while simultaneously increasing exposure to data misuse.

---

[462] V V Giri National Labour Institute, *Gig and Platform Workers: Vision Towards Social Protection in India* (VVGNLI 2021).

[463] The Cashless Revolution *The Cashless Revolution: China's Reinvention of Money and the End of America's Domination of Finance and Technology* (Oxford University Press 2020).

[464] Re-Engineering India *Re-Engineering India: Technology Solutions for the World's Largest Democracy* (Penguin Books India 2015).

3.4.Role of Digital Literacy

Another factor worth mentioning that adds complexity to the situation is that of digital illiteracy. Indeed, it can be said without exaggeration that the informal workers will be completely unfamiliar with any form of digital technology before undertaking their job. This implies that such people have no clue as to:

- Distinguishing legitimate emails from phishing emails.
- Making sure that their personal data remains secure.
- Safely logging into their accounts.
- Devising solutions to digital conflicts.

Without this foundational knowledge, workers are unable to safeguard themselves against cyber threats. Digital tools, instead of empowering them, can become instruments of exploitation.

4. Structural and Institutional Challenges

The cybersecurity dangers faced by informal and contractual employees go further than personal risks because of their connection to systematic vulnerabilities within the system as a whole. The cybersecurity threats posed to informal and contractual employees can be linked to systematic failure, which has led to these employees being marginalized in cyberspace.

4.1. Digital Illiteracy and Knowledge Gaps

The second issue that emerges regarding the process of adoption is connected with the lack of digital skills among the workers. On the one hand, the workers should learn to operate in the digital space and become accustomed to performing certain tasks online and earning money online due to their lack of skills, but not as a result of being well-prepared. In spite of the fact that nowadays most individuals make transactions and use different services via smartphones and applications, they know very little about creating secure passwords, two-factor authentication, protecting themselves from cyber threats, and securing personal data.

Specifically, since workers are unaware of such threats as sending OTP codes, clicking on malicious links, and installing malware, they are vulnerable to various types of cyber-attacks.

4.2. Absence of Accessible Grievance Redressal Mechanisms

Another key issue that emerges is the absence of an effective channel through which such complaints can be filed. In the informal sector, employees are unaware of how to file a complaint with regard to cyber-fraud, cyber identity theft, and cyber harassment. There may be a cybercrime help line, but it would not be easily accessible to them.[465]

---

[465] Centre for Internet and Society, *Privacy, Security and Digital Inclusion in India* (CIS Report).

Apart from that, the process of receiving compensation for the damages suffered is both time-consuming and demanding, which explains why workers do not take this route. In most cases, people who fall victim to cybercrimes prefer to accept their destiny rather than fighting back for justice, since it would be less troublesome.

4.3. Informality and Lack of Employer Accountability

The employment contract is a cause of cyber-crime through a number of lenses. It must be noted that certain obligations lie on the employer's part when it comes to maintaining secrecy concerning confidential information and creating a safe work environment for the worker. However, the employment contract loses its relevance and essence when the employer-worker relationship remains informal in nature and the duties of the former towards the latter are nonexistent.

When it comes to remote employment, the online service providers replace the employer in the context of their mutual interaction and thus, any obligations they have towards the employee become binding and meaningless. Therefore, there is no sense of accountability remaining from the perspective of the online service provider, while the burden of obligations lies solely on the employee's part.[466]

4.4. Technological Inequality and Access Constraints

The technology gap creates more chances of cybercrime. The informal labour is forced to rely on less sophisticated devices such as low-cost cell phones and outdated software. Besides, they might have to share computers that do not have adequate security measures in place. The problem of not having secured internet and wireless services further complicates the situation especially when using free Wi-Fi services.

Moreover, because of their financial constraints, such informal labourers are unable to afford sophisticated technological devices as well as anti-virus programs.

5. Digital Vulnerabilities and The Precarity of Informal Workers

Digital vulnerabilities translate into economic loss, social harm, and legal exclusion, reinforcing the precarious position of such workers in the digital economy.

5.1. Gig Workers and Fraudulent Digital Interfaces

Delivery drivers, chauffeurs, and freelancers depend greatly on the use of mobile applications when they search for gigs that offer them income. This dependency may be abused by hackers since the trust that gig workers have on mobile applications can provide them with a loophole in gaining access to the gig workers' personal information.

---

[466] Ministry of Electronics and Information Technology (MeitY), *Annual Report* (Government of India).

There have been instances wherein gig workers receive calls from fraudsters who pose as members of the platform that gig workers use. They trick the victims into signing in to a fraudulent website or updating their login details to install a new version of the application. This causes the gig workers to divulge their login details and even the one-time password.[467]

Algorithmic management in the gig economy is highly straightforward and ruthless. The vast majority of gig workers depend on their daily wages. Therefore, anything that would disrupt them negatively could include low morale, additional costs, or even the alteration of algorithms. The situation becomes much more complicated due to the lack of responsibility at the level of the platform. Once the gig worker is impacted by some form of misconduct on the part of the platform, he will not be able to recover his losses.[468]

It has become clear from the case of All India Gig Workers Union vs. Union of India, where there have been questions about the implementation of workers' rights and handling the pandemic situation. The matter of lack of accountability of such platforms, along with their arbitrariness regarding income earned by gig workers, has come to light.[469]

5.2. Domestic Workers and Fake Job Portals

Today, there are numerous individuals searching for work through online platforms and social media channels. Although these platforms provide the best opportunity for finding jobs, they are also the places where these individuals can be easily fooled by scammers.

The scammers would offer jobs that pay well and have acceptable working conditions, but these would come at a price in terms of application costs and personal data sharing. Some of these helpers could get involved in money laundering schemes, while others could become victims of human trafficking.

Due to the unsatisfactory nature of the method adopted for verifying such transactions and the ignorance among the employees, there will obviously be numerous cases of deception and frauds. This is because they don't fall under the organized sector, therefore not covered by any law. Privacy rights are included within the broader ambit of privacy rights as mentioned by K.S. Puttaswamy (Aadhaar) vs. Union of India. In supporting the constitutional validity of the Aadhar scheme in India, the apex court in its judgment states that the need for regulating the use of such information shall be proportionate. Employees using the Aadhar card as their mode of payment face various difficulties, including non-payment of salary due to mismatched biometrics and misuse of information.[470]

Rather, the increasing phenomenon of implementing surveillance management systems in digital companies poses grave issues regarding challenges to the freedom and independence of employees. The monitoring of surveillance can occur via methods such as surveillance on mobile applications, geo-tracking, and measuring performances, which form what is known as the "digital panopticon."

---

[467] Telecom Regulatory Authority of India (TRAI), *The Indian Telecom Services Performance Indicators* (TRAI Report).
[468] Unique Identification Authority of India (UIDAI), *Annual Report* (Government of India).
[469] Aparna Ravi, 'Regulating the Gig Economy in India: Platform Work and Labour Rights' (2022) *NUJS Law Review*.
[470] Janaki Srinivasan and others, *Digital Identity and Inclusion in India* (IT for Change 2018).

This continuous act of surveillance may be harmful to the fundamental rights of humans safeguarded by Article 21 of the Constitution of India in the case of Francis Coralie Mullin v. Administrator, UT of Delhi.[471]

5.3. Gendered Cyber Harassment and Online Abuse

Nevertheless, the individuals employed within the informal sector remain vulnerable to a number of cybercrimes due to the fact that they use computers in order to behave professionally or advertise their services.

For example, when women use social networking sites or instant messaging services in order to market their products, they may be subject to harassment and intimidation from the consumers. Additionally, their personal data could be misused without their permission. These activities can have adverse implications but women cannot demand justice since they lack knowledge about the law.

6. Towards an Inclusive Cybersecurity Framework

The implementation of a cyber security framework that will ensure that the interest of the informal workers will be included must go beyond theory and seek ways through which such a measure can actually be enforced among the informal workers. The framework does not only have to reduce cyber risk, but it must achieve a shift in power dynamics within the digital economy dominated by the informal workers.

6.1. Digital Literacy and Awareness

A further point that needs consideration here is that digital literacy among informal and contractual workers cannot just be seen as a one-way learning experience. Rather, digital literacy must be considered an ongoing process that considers changes to technology, platforms, and also the issue of cybersecurity. The point is that in today's day and age, with informal and contractual workers becoming increasingly dependent on the mobile workplace, digital security emerges as a very important aspect of workers' rights.[472]

6.2. Localized and Contextual Training Design

It is imperative for the digital literacy training program to start from a practical base. The majority of the current digital literacy training programs are bound to collapse because they have taken a very impractical stance. It would help if the training incorporated situations which might arise in the utilization of digital tools such as fraudster calls made by customers, fraudulent job opportunities posted on social media platforms, phishing emails regarding payments, and UPI and OTP scam cases.

In terms of accessibility, it is not enough for the training to be translated into regional languages; it must also be accessible through other means of communication like visually and auditory-based communications. Examples of such training content include short films, infographics, and story-based

---

[471] The Age of Surveillance Capitalism *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).
[472] Centre for Internet and Society, *Digital Literacy, Privacy and Inclusion in India* (CIS Report).

modules because most of the employees are uneducated. Micro-learning modules, which contain information for 2 to 5 minutes, will be appropriate alongside application-based communication.[473]

6.3.Behavioural Change Approach

Knowledge alone will not guarantee the employees' safety when performing online operations. For instance, even though the workers know everything that threatens their information security, they will still suffer from the effects of the circumstances due to their urgent need for money or because they have a habit of sending emails. Based on this reasoning, digital literacy should be able to cover the understanding of behavioural learning.

There are two approaches that could be used to address this challenge. First, the application can send text reminders to remind the employees that they have to safeguard their credentials and should never send any one-time passwords. Secondly, pop-up notifications can be placed on the screen to alert the workers that certain activities, such as sharing passwords, are unacceptable.

It is crucial to note that when designing these strategies, one fundamental issue must be considered. The problem relates to the economic insecurity of the employees. To this end, it is vital to ensure that the messages sent to the employees are friendly.

6.4. Recognition of Digital Labour Rights

One other aspect that should be taken into account during the process of reform is that of incorporating informal and gig workers as digital persons that should be accorded the legal rights under data security and cybersecurity legislation. At the moment, the legislation only views them as consumers and contractors.[474]

It is possible to achieve recognition in this regard through the following means:

- Control rights for the information produced by the workforce within the platform economy.
- Right to consent to how the information produced by them is used within the platform economy instead of consenting to the lengthy and difficult-to-understand terms and conditions of the agreement.
- The right to defend oneself against any form of abuse by algorithms, such as deactivating one's account, discriminatory task assignment, or automatic pay cut.

In summary, the above mentioned new perspective will bring about worker recognition within the digital labour market.

---

[473] The Age of Surveillance Capitalism *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).
[474] Software Freedom Law Center, *Privacy, Surveillance and Data Protection in India* (SFLC Report).

6.5. Specialized Redressal Mechanisms

One of the main shortcomings of the present-day mechanism is that there exists no suitable platform for airing their complaints in case of any losses suffered owing to the online process.

One of the important aspects that need to be taken into account when considering the current legal structure is the lack of an effective procedure for dealing with complaints about cybercrimes against informal sector employees. These can include fraud, hacking, embezzlement of wages, identity theft, and other similar crimes.

In this respect, the other significant aspect will be the establishment of a grievance cell at the district and regional levels dealing with problems associated with cyberspace and serving the interests of the workers engaged in the gig economy. In this respect, it will become imperative to ensure that:

- The disputes pertaining to small amounts of money including UPI frauds and salaries are dealt with in a timely manner.
- The grievance cells are available to workers using mobile apps and toll-free numbers.
- The process has an easy access to banks and companies providing platforms for a speedy settlement of disputes.

It will be equally vital to ensure that the workers find it easier to file their grievances.

7. Platform Accountability (From Voluntary to Enforceable Responsibility)

Considering the increase in digital job opportunities, it is important to understand that these websites are not intermediaries anymore; they are quasi-employers. It is important, therefore, to regulate these websites, especially when it comes to accountability, because this will ensure that these sites take responsibility for cyber security.[475]

7.1. Algorithmic Transparency and Explainability

An essential element of platform accountability concerns the transparency of decisions made by algorithms that affect the livelihoods of those who rely on the services offered by these platforms. As it stands today, most gig and digital platforms use opaque algorithms to assign tasks, rate performances, and deactivate accounts.

It will be important for the right to an explanation of any decision that might have been made concerning the worker by the algorithm. These explanations shall entail:

- Explanation of the reasons for the modifications done on their scores
- The rationale for allocating certain tasks and assigning their priorities
- The reason certain accounts may have been either suspended or terminated by the platform

[475] Uma Rani and Parminder Jeet Singh, 'Digital Labour Platforms and New Forms of Informality: The Case of India' (2020) *Indian Journal of Labour Economics*.

- The data fed to the algorithms that help make automatic decisions

In addition, there ought to be compulsion on the part of the platform to issue regular transparency reports on the operations of the algorithm and the type of data utilized.

7.2. Built-in Security by Design

However, there needs to be some proactivity in ensuring cybersecurity of the digital work systems apart from the reactiveness of implementing these features where these will have been embedded in the process of designing. In this way, it will be possible for them to be included in the digital work system through the 'security by design' principle.[476]

A number of security features that should be considered are:

- Automated system that detects any fraudulent activity within the system, including those relating to payment, hacking into other accounts, or suspicious logins
- Increased measures of security, including MFA to prevent any unauthorized access to the system
- Security alerts on any suspicious payments, links, or identity verification

Such safeguards should not be optional add-ons but statutory compliance requirements, ensuring that digital labour platforms are designed with worker safety as a core structural principle rather than an afterthought.

7.3. Liability and Compensation Mechanisms

One of the major drawbacks of the present platform governance architecture is the lack of liability structures in case of any digital harm caused. This implies that the burden of all expenses will fall on the shoulders of the user, but in reality, it is the users who depend solely upon the platform system for their earnings.

Reforms should make it necessary for there to be some shared liability on the part of the platform specifically in instances where:

- There is exploitation of the vulnerabilities in the system for either accessing or committing fraud.
- Lack of responsibility on the platform results in data breach or compromise of accounts.
- Algorithmic or technical failures directly result in income loss

---

[476] Rahul Matthan, 'Beyond Consent: Data Protection and Platform Responsibility in India' (2020) *Indian Journal of Law and Technology*.

In such cases, the platform should be in a position to offer compensation for the losses that arise from the above cases, particularly the loss of income through loss of wages, restoration of accounts, and financial help in the interim.[477]

7.4. Worker Representation in Governance

The implementation of governance through platforms will not yield positive results without the participation of workers within such systems. At present, almost all decisions relating to security and associated issues within the operations of platforms are made by corporate executives, who do not necessarily include workers.

It is thus imperative that platforms ensure the involvement of workers in their policy-making processes, particularly through advisory boards or similar entities, which will aid:

- In ensuring the development of cybersecurity policies based on practical on-ground situations
- Building feedback mechanisms for the emergence of new risks
- The establishment of legitimacy within the process of governance

This cooperation allows the transition from regulatory to collabourative governance models.

The transition from self-regulation to mandatory responsibility of platforms would be important for the development of digital economy. Transparency of algorithms, the security-by-design concept, responsibility, and the involvement of representatives of the worker's voice give an opportunity for the platforms to rise above being merely service providers, but also assume the responsibility for defending the interests of the workers. This becomes crucial, as innovation must not substitute insecurity and inequality, especially absence of basic labour rights.

8. Institutional Support (Building an Ecosystem of Protection)

However, any form of protection of either informal workers or contractual employees working within the digital sphere would not be achieved through a fragmented approach. It would be important that such an approach be comprehensive and involve all aspects of support including the local aspect, the technological aspect, the regulatory aspect, and the corporate aspect. This would ensure that there is security in the digital environment equal to that found in the workplace.[478]

8.1. Decentralized Support Structures

It is absolutely essential that the present system should fail to create any sort of access point to educate and gig workers, who suffer from cyber crime at a grass-root level. In fact, most of them might be

---

[477] NITI Aayog, *India's Booming Gig and Platform Economy* (Government of India 2022).

[478] Aparna Ravi, 'Regulating the Gig Economy in India: Platform Work and Labour Rights' (2022) *NUJS Law Review*.

lacking in terms of knowledge, expertise, and even time to go to the central office of cybercrime and court.

As such, it becomes absolutely essential to create cyber assistance centers in different communities or localities, which include:

- Cyber community centers or cyber facilitation centers, in collabouration with the labour department.
- Cyber help desks, where the basic complaints of people related to cyberspace could be listened to.
- Mobile cyber assistance centers, through which assistance could be rendered to informal workers' organizations such as markets, construction sites, and transportation points.

The importance of such centers lies in the fact that they should be free, multilingual, and made possible through professionals. It is only through this method that less-educated labourers or those who do not know how to use computers can use such centers without relying too much on the conventional legal system.

8.2. Public-Private Partnerships (PPP Model for Cyber Protection)

Considering the multisectoral characteristics of digital labour, it becomes vital that the institution fosters collabouration between government agencies and the non-government private sectors. Public-private partnerships may play a pivotal role in implementing security measures that are scalable in nature.

- The telecom sector can offer automatic alerts with regard to any phishing attacks, scamming attempts, or even malicious hyperlinks.
- The banking and payments sector may develop easy-to-implement procedures for rectifying any fraud.
- The digital labour platform providers can provide risk data anonymously to the regulatory authorities for identifying any cyber fraud.
- NGOs may assist in awareness creation and grievances management.

The collabourative relationship facilitates sharing resources, technology innovations, and quick action, thus ensuring that the security of cyberspace does not rest in the hands of only the government.

8.3. Strengthening Cybercrime Infrastructure

The efficiency of these institutions depends greatly on the competence and effectiveness of the agencies tasked with enforcing the law and tackling cybercrime. However, despite their existence, the

existing structures do not take into consideration the vulnerabilities of the informal workers since they experience cyber-fraud all the time.[479]

- Training of police officers in dealing with cyber crimes concerning gig workers and informal cyber crimes relating to their employment with due regard and consideration
- Exclusion of the bureaucracy involved in the process of lodging complaints, which serves as a deterrent in filing complaints
- The process of responding promptly, particularly when cyber fraud occurs in finance, which is vital for daily subsistence and existence
- Cyber cells devoted to cases of cyber crimes in relation to labour

Additionally, integrating cybercrime reporting with labour departments and financial regulators can create a coordinated enforcement ecosystem, reducing fragmentation and improving recovery outcomes for victims.

8.4. Inclusion through Design (Human-Centred Digital Infrastructure)

The inclusion of technology must also come into play when creating the technology so that the technology does not marginalize the very workers who utilize the technology. This means that the inclusion must become inherent in the architecture of the platform being used.

- Simplistic interface design that would prevent the technology from excluding workers with limited literacy levels
- Multi-language support for regional languages and voice-based interfaces for illiterate workers
- Ideas to make navigation easier by way of icon and voice-based navigational systems
- Safeguarding the workers with low literacy levels through simplified security systems with a fraud alert and simple authentication process

Nevertheless, most importantly, the systems should never make any assumptions about the prior technical knowledge of their users, and should design the process of safety in such a way as to be easy for them to understand and utilize.

On the other hand, the institutional response towards both digital workers and informal economy workers should stop being merely supportive and start being protective by incorporating local support, inter-sectorial collabouration, enforcement, and technology design into itself. When all four strategies are combined at once – decentralization, PPPs, cybersecurity, and human-centered design – the result becomes a highly effective institutional response framework that will protect the workers, not only themselves.[480]

---

[479] Internet Freedom Foundation, *Cybersecurity and Data Protection in India: Gaps and Challenges* (IFF Report).
[480] Ministry of Electronics and Information Technology (MeitY), *Digital India Programme: Annual Report* (Government of India).

9. Conclusion

The right cybersecurity approach is not to be considered just as an approach helping to protect the users of the system. In fact, there is an increasing number of informal workers, contractors using different platforms, technological supply chains and other services on a daily basis. Even though they play an important part in the process, their role is legally invisible. We have come up with the scenario where people using digital technology become defenseless. It becomes obvious that there is a need to make certain changes within the framework of cybersecurity policy. The traditional policy assumes that everyone should be concerned about his or her own cybersecurity when using the network. This way of tackling the problem is clearly doomed to failure as it refers to the uneducated people whose negotiating positions are far weaker than those of the platform owners.[481]However, a correct approach to cybersecurity cannot be viewed as something meant to help the users of the particular system. Rather, it is necessary to note that today many informal workers, contractors hired by several platforms, technological chains of production and other similar groups operate in various fields. Although these groups are crucial to this process, their participation goes unseen from the perspective of law. Regarding the situation at hand, one can say that the participants in this process using digital technologies have no security at all. Therefore, it is evident that some measures should be undertaken to deal with the issues associated with cybersecurity. To begin with, the traditional policy implies that every person should realize his or her problems regarding cybersecurity when working on the network. Nevertheless, such an approach would not bring the desired results as the members of this group are much less educated than the owners of the platforms are.[482] Another equally important group of stakeholders is civil society organizations, academic institutions, and advocacy groups. Apart from simply increasing awareness, this includes rights-based advocacy, policy monitoring, legal literacy education, and organizing workers. Such stakeholders act as intermediaries, ensuring that when there is any conversation taking place around policy development, it does not stay only within the realm of theory but takes into account the practicality of the situation in the workforce. What is even more important is the need to re-conceptualize the informal and contractual workforce as stakeholders within the same ecosystem. In effect, empowerment means that they should get the right knowledge of their rights and be involved in governance mechanisms. Last but not least, cybersecurity should be made a core element of an integrated and converged architecture that embraces labour rights, social protection, financial inclusion, and digital governance in order to address the inherent shortcomings of informal and gig workers. In other words, the idea of cybersecurity should change from self-protection to something more proactive, where cybersecurity is used in order to guarantee equality and inclusiveness in a way that ensures that digital transformation will not exacerbate inequalities but will help resolve them.

----------**********----------

[481] Rahul Matthan, 'Beyond Consent: Data Protection and Platform Responsibility in India' (2020) *Indian Journal of Law and Technology*.

[482] Kunal Sen and Ravi Kanbur, 'Informality in India: Causes, Consequences and Policy Responses' (2015) *Indian Journal of Labour Economics*.

Chapter 19
Guardians of the Grid: Conceptual Frameworks of Modern Cyber Security

*Ankita Mukherjee, Assistant Professor, School of legal studies, Swami Vive*kananda University

Abstract

The rapid expansion of digital technologies has fundamentally transformed contemporary society, creating both unprecedented opportunities and complex security challenges. Cyber security has emerged as a critical discipline aimed at safeguarding digital infrastructure against evolving threats. This paper examines the conceptual foundations of modern cyber security, focusing on its core principles, key frameworks, legal and governance structures, and emerging challenges. It critically analyses foundational models such as the CIA Triad, the NIST Cybersecurity Framework, and ISO/IEC 27001, while also exploring contemporary approaches such as Zero Trust Architecture. The study further evaluates the legal framework in India, particularly the Information Technology Act, 2000, and the institutional role of CERT-In. By integrating theoretical insights with practical considerations, the paper highlights the need for a resilient, adaptive, and interdisciplinary approach to cyber security in an increasingly interconnected world.

Keywords: *Cyber Security; CIA Triad; NIST Framework; ISO 27001; Zero Trust; Cyber Law; Information Technology Act; Digital Governance; Cyber Risk; India.*

Introduction

The twenty-first century has been characterized by an unprecedented proliferation of digital technologies, fundamentally reshaping the structure and functioning of contemporary society. Critical sectors such as governance, finance, healthcare, and education are now deeply embedded within complex networks of interconnected information systems. While this transformation has yielded significant gains in efficiency, accessibility, and innovation, it has simultaneously introduced a range of systemic vulnerabilities. In this context, cyber security has emerged as an indispensable prerequisite for sustaining trust, resilience, and stability within the digital ecosystem.

Cyber security is conventionally defined as the protection of systems, networks, and data against unauthorized access, disruption, or destruction. However, such a definition captures only its technical dimension. In its broader sense, cyber security constitutes a multidisciplinary field that intersects with law, public policy, economics, and behavioral sciences. It encompasses not merely the implementation of technical safeguards but also the governance of risk, the allocation of responsibility, and the establishment of accountability within digital environments.

In the Indian context, the accelerated pace of digitalization—driven by initiatives such as Digital India, the expansion of digital financial services, Aadhaar-enabled platforms, and e-governance systems—has significantly heightened the relevance of cyber security. This expansion has been accompanied by a corresponding increase in cyber-related offences, including phishing, identity theft, ransomware attacks, and financial fraud. At the global level, cyber threats have assumed the character of national security concerns, with the growing prevalence of cyber warfare, state-sponsored attacks, and transnational cybercrime networks.

Against this backdrop, the present chapter seeks to examine the conceptual frameworks that underpin modern cyber security. It critically analyses foundational principles, institutional and technical frameworks, legal and regulatory structures, and emerging challenges. By integrating theoretical perspectives with practical considerations, the chapter conceptualizes cyber security as a form of systemic guardianship over the digital domain.

Conceptual Foundations of Cyber Security

Meaning and Scope

Cyber security encompasses a wide range of practices and technologies designed to safeguard digital assets. It includes multiple subdomains:

- Network Security: Protection of network infrastructure from unauthorized access and misuse.
- Information Security: Protection of data integrity and confidentiality.
- Application Security: Ensuring that software applications are secure from vulnerabilities.
- Operational Security: Management of processes and decisions related to data handling.
- End-User Education: Training users to recognize and avoid cyber threats.

The scope of cyber security extends beyond prevention to include detection, response, and recovery. It is not only about stopping attacks but also about minimizing damage and ensuring continuity of operations.

Core Principles: The CIA Triad

The conceptual foundation of cyber security is built upon three fundamental principles collectively known as the CIA Triad:

- Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals. Techniques such as encryption, secure passwords, and access control mechanisms are used to protect confidentiality. For example, banking systems use encryption protocols to safeguard customer data from unauthorized access.

- Integrity

Integrity refers to the accuracy and consistency of data. It ensures that information is not altered or tampered with without authorization. Mechanisms such as hashing, digital signatures, and checksums help maintain data integrity. For instance, any unauthorized modification of financial records would violate the principle of integrity.

- Availability

Availability ensures that information and systems are accessible when needed. This involves maintaining system uptime, implementing backups, and protecting against denial-of-service attacks. For example, e-commerce platforms must ensure continuous availability to serve customers effectively.

Extended Principles of Cyber Security

While the CIA Triad forms the foundation, modern cyber security incorporates additional principles:

- Authentication: Verification of user identity through passwords, biometrics, or multi-factor authentication.

- Authorization: Determining the level of access granted to authenticated users.

- Non-repudiation: Ensuring that individuals cannot deny their actions, often achieved through digital signatures.

- Accountability: Tracking user actions to ensure responsibility for activities within a system.

- Resilience: The ability of systems to withstand and recover from cyber incidents.

These principles collectively ensure a comprehensive approach to securing digital environments.

Key Cyber Security Frameworks

Cyber security frameworks provide structured methodologies for managing risks and implementing security controls. They help organizations align their security practices with established standards.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is widely appreciated for its flexibility and practical applicability across different types of organizations. It provides a structured yet adaptable approach to managing cyber security risks.

Core Functions:

- Identify:
- Understand organizational assets, systems, and data
- Assess risks and identify vulnerabilities

Protect:

- Implement safeguards such as access controls and encryption
- Conduct employee training and awareness programs

Detect:

- Monitor systems continuously
- Identify potential cyber incidents at an early stage

Respond:

- Take immediate action to contain threats
- Minimize damage and manage communication

Recover:

- Restore systems and services after an incident
- Improve resilience and prevent future occurrences

Key Components:

- Systematic Risk Assessment
- Identify threats and evaluate their impact
- Implementation of Security Controls
- Apply appropriate technical and organizational measures
- Continuous Monitoring and Improvement
- Regularly review and update security practices

Significance:

- Ensures structured protection of sensitive information
- Demonstrates compliance with international standards

Zero Trust Architecture

Zero Trust Architecture represents a modern approach to cyber security that challenges traditional assumptions of trust within a network.

Core Principles:

- Never Trust, Always Verify
- Assume threats may exist both inside and outside the system

Key Features:

- Continuous Verification
- Authenticate users and devices at every stage
- Least Privilege Access

- Provide only necessary access rights
- Micro-Segmentation
- Divide networks into smaller, secure segments
- Strong Identity Management
- Maintain strict control over user identities and access
- Relevance
- Highly suitable for cloud computing and remote work environments

Risk Management Frameworks

Risk management is a fundamental aspect of cyber security, focusing on identifying and managing potential threats effectively.

Key Steps:

- Risk Identification:
- Detect possible threats and vulnerabilities
- Risk Assessment
- Evaluate likelihood and impact of risks
- Risk Mitigation
- Implement strategies to reduce or control risks
- Continuous Review
- Update measures based on evolving threats
- Importance
- Ensures efficient use of resources
- Helps prioritize critical security concerns
- Supports informed decision-makin

Legal and Governance Dimensions

Cyber security cannot be effectively implemented without a strong legal and institutional framework. Laws and policies define acceptable behavior, establish penalties for violations, and provide mechanisms for enforcement.

Indian Legal Framework

The cornerstone of cyber law in India is the Information Technology Act, 2000. The Act provides legal recognition to electronic records and digital signatures while addressing various cyber offences, including:

- Hacking and unauthorized access
- Identity theft and impersonation
- Cyber terrorism
- Data breaches

Amendments to the Act have expanded its scope to include data protection and intermediary liability. Despite its significance, the Act faces criticism for being outdated in certain aspects, particularly in addressing emerging technologies.

Institutional Mechanisms

The CERT-In serves as the national nodal agency for responding to cyber security incidents in India. Its functions include:

- Issuing alerts and advisories
- Coordinating incident response
- Promoting cyber awareness

Additionally, the National Critical Information Infrastructure Protection Centre (NCIIPC) focuses on protecting critical sectors such as energy, banking, and telecommunications.

International Cooperation

Cyber threats often transcend national boundaries, making international cooperation essential. Organizations such as the United Nations and regional alliances work toward establishing norms for responsible behavior in cyberspace. However, differences in national interests and legal systems pose challenges to global governance.

Emerging Trends and Challenges

The dynamic nature of technology continuously reshapes the cyber threat landscape.

Artificial Intelligence and Cyber Security

Artificial intelligence (AI) enhances cyber security by enabling advanced threat detection and automated responses. However, it also empowers attackers to develop sophisticated techniques such as deepfakes and automated phishing campaigns.

- Cloud Computing

Cloud computing offers scalability and cost efficiency but introduces challenges related to data privacy, shared responsibility, and misconfiguration risks. Organizations must adopt robust security practices to mitigate these risks.

- Internet of Things (IoT)

The proliferation of IoT devices has expanded the attack surface. Many devices lack adequate security features, making them vulnerable to exploitation. Compromised devices can be used in large-scale attacks such as botnets.

i. Cyber Warfare and National Security

Cyber warfare has emerged as a significant component of modern conflict. State-sponsored attacks target critical infrastructure, financial systems, and government institutions. These threats highlight the need for robust national cyber security strategies.

ii. Human Factor in Cyber Security

Human error remains one of the leading causes of cyber incidents. Phishing attacks, weak passwords, and lack of awareness contribute to vulnerabilities. Therefore, user education and training are essential components of cyber security.

Critical Analysis of Cyber Security Frameworks

While existing frameworks provide valuable guidance, they are not without limitations:

i. Fragmentation

The existence of multiple frameworks can create confusion and overlap, particularly for organizations operating in different jurisdictions.

ii. Implementation Challenges

Many organizations struggle to translate theoretical frameworks into practical measures due to resource constraints and lack of expertise.

iii. Rapid Technological Change

Cyber security frameworks often lag behind technological advancements, making it difficult to address emerging threats effectively.

iv. Overemphasis on Technology

Excessive focus on technical solutions may overlook human and organizational factors, which are equally important.

Need for Interdisciplinary Approach

Effective cyber security requires collaboration across disciplines, including law, technology, and social sciences. Cyber security has become a foundational element of modern society, underpinning the

functioning of digital infrastructures across sectors. The conceptual frameworks examined in this chapter provide a structured basis for understanding and managing cyber risks.

However, the dynamic nature of cyberspace necessitates continuous adaptation and innovation. Legal systems must evolve in tandem with technological advancements, while organizations must adopt flexible and resilient strategies. Ultimately, cyber security extends beyond technical considerations; it represents a collective responsibility aimed at preserving trust and stability in the digital age. As "guardians of the grid," stakeholders must collaborate to ensure that the benefits of digital transformation are realized without compromising security or privacy.

----------**********----------