Information Resilience in the Artificial Intelligence Era: A Global Scenario of Cybersecurity Strategies

Subhadip Mandal Kanu Chakraborty Swapan Kumar Patra
Navin Upadhyay Anisha Kumari

Abstract

In the AI era, there is a constant push and pull between cyber attackers and defenders to create a resilient information system. Some popular big AI giants like Open AI, Google, Microsoft etc and many developed nations such as UK, USA, Singapore etc are working on Cyberattacks. This paper is a review of the policy statements adopted by selected governments and the subsequent policy measures taken by the big multinational corporations. This study adopts a qualitative and descriptive research methodology based on secondary data analysis. The approach is primarily documentary and policy review-based, aiming to explore how various national and international entities are addressing cybersecurity challenges in the context of growing Artificial Intelligence adoption. With this growing use, there is a major apprehension about the safety, security, integrity, and robustness of the information system. So, it is a matter of concern how the information system deals with this issue. This study highlights the impact of AI in modern information resilience systems and focusing on the way to enhance their ability to handle uncertainties, adversarial attacks, and data perturbations.

Keywords: Artificial Intelligence, Cyber Laws, Cybersecurity, Information Resilience

1. Introduction

The term "Artificial Intelligence" (AI) was coined by McCarthy in 1956 while he was preparing for the 1956 Dartmouth Conference (McCarthy et al., 2006). The term AI denotes the theory of human intelligence being exhibited by machines (Helm et al., 2020). In the current era of exponential growth of "big data" and rapid technical innovation, AI has made an unparalleled leap from theory to practical application. AI made significant impact on every domain like healthcare to finance, and from autonomous vehicles to cybersecurity (Kühl et al., 2022).

National Institute of Standards and Technology (NIST), US Department of Commerce, defines Information Resilience as "The ability to maintain required capability in the face of adversity" (CSRC Content Editor, n.d.). Further NIST defines Information System Resilience as "The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while

Corresponding Author
Kanu Chakraborty
Email: kchakraborty.lib@iitbhu.ac.in

maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs" (CSRC Content Editor, n.d.).

In the context of AI and ML systems, information resilience encompasses the capacity to withstand various challenges associated with data quality, security vulnerabilities, concept drift, domain shift, and ethical considerations, while still achieving reliable and trustworthy outcomes. The importance of information resilience in AI systems cannot be overstated, particularly in today's data-driven globalized world, where these technologies play integral roles in decision-making processes across various domains. This study analyses the concept of information resilience in artificial intelligence and Machine learning environments, looking at strategies to enhance their ability to withstand uncertainties, adversarial attacks, and data perturbations.

2. Literature Review

In the field of artificial intelligence (AI) and cybersecurity, information resilience is influenced by several key factors that helps the organizations to recover from cyber threats, surprise attack, unexpected changes etc. These key factors include the AI tools and technologies, the need for proactive awareness, and creating the proper robust governance frameworks. Alnaffar (2024) reveals that contributing to information resilience in AI and cybersecurity includes staying aware, teach people early, collaboration among stakeholders, continuous learning, and robust governance rules to address emerging risks and vulnerabilities associated with the integration of AI technologies. There was a need for robust governance frameworks to address AI challenges. Sontan and Samuel (2024) analyze the key factors contributing to information resilience in Artificial intelligence and cybersecurity. These include the automated vulnerability analysis, advanced threat detection, quick response, and the implementation of ethical rules. Emerging trends like adversarial machine learning and zero-trust security further enhance resilience against evolving threats. Authors are concerned about ethical and privacy concerns in AI deployment, and the importance of responsible decision-making and transparency. Laksito et al. (2025) explained that the data protection rules and regulations differ between countries, impacting the development and implementation of AI technologies. The General Data Protection Regulation focuses on individual rights by requiring clear information for data processing. It sets a high standard for data protection, influencing global norms. Lourens et al. (2022) emphasize that information resilience enhances through the AI technologies by using intelligent models to identify malware, data breaches, and network attacks. The author suggests that AI strengthens cybersecurity against advanced cyberattacks by defending against various security threats. However, there are some limitations, such as Practical issues and difficulties in AI integration. Current traditional cybersecurity systems are not sufficient to defend against advanced cyber-attacks. In contrast, China's "Personal Information Protection" and Japan's Act on the "Protection of Personal Information" adopt more flexible approaches, balancing innovation with privacy needs. This flexibility allows for rapid adaptation to technological advancements.

3. Objectives:

- To critically analyze the global cybersecurity policies and strategies used by international organizations and leading nations.
- To examine the contribution of AI and ML technologies in strengthening information resilience and reducing cyber threats across the different sectors.
- To investigate the challenges and opportunities in adopting AI based cybersecurity frameworks.

4. Methodology/Approach

This study adopts a qualitative and descriptive research methodology based on secondary data analysis**.** The approach is primarily policy review-based analysis, aiming to explore how various national and international entities are addressing cybersecurity challenges in the context of growing Artificial Intelligence adoption. Data collected from official government policy documents and resolutions (e.g., UN AI Resolution, US Executive Orders, and India's Cybersecurity Policy), reports and publications from international organizations (e.g., ITU, Budapest Convention), strategy documents from multinational corporations (e.g., Microsoft, Apple, OpenAI), peer-reviewed literature, and publicly available whitepapers.

5. Information Resilience and Cybersecurity

AI-driven resiliency augmented by ML components provides a powerful framework for building robust systems that can adapt to challenges, recover from disruptions, and continue functioning effectively. In this context, the purpose of this paper is to capture the role of AI & various policy issues and strategies in the Cybersecurity framework globally. By definition, "Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies" (Cyber Security, n.d.). It encompasses various measures to defend against cyber threats, including network security, data security, and endpoint security. AI and ML algorithms can analyse patterns in data to identify abnormal behaviour that can point to a security risk. AI can automate certain aspects of incident response, enabling faster and more efficient reactions to security incidents. Automated responses can include isolating affected systems, blocking malicious activities, and notifying relevant personnel.

Information resilience means the ability to recover from misinformation and disinformation. Libraries play a pivotal role by offering verified, curated, and timely information that helps the communities resist misinformation and disinformation. Libraries provide trusted sources, promote information literacy, and educate users to find the proper resources, helping to combat misinformation. Libraries are acting as community hubs that connect people to support networks, resources, and help people during a crisis.

The sharp rise in cyber attacks across sectors underscores the urgency of collective action. Libraries, as trusted public institutions, can contribute by promoting information literacy program, and awareness campaigns to help communities to understand the risks such as phishing, identity theft, and disinformation. Achieving this requires coordinated policies, collaborative stakeholder engagement, and the development of sustainable cybersecurity solutions that protect both institutional data and the rights of users.

5.1 Strategies for Information Resilience

Organizations carry out thorough risk assessments to find possible weak points and threats (IT Governance Ltd, 2013). This involves understanding the threat landscape, assessing potential impacts, and prioritizing risk mitigation strategies. Robust cybersecurity practices form a crucial component of information resilience (Landoll, 2021). Implementation of firewalls, intrusion detection systems, and encryption technologies safeguards information assets from unauthorized access and cyber threats. Regular data backups and efficient recovery mechanisms safeguard against data loss (Van Den Adel et al., 2021). This includes automated backup solutions, off-site storage, and streamlined recovery processes. Information systems designed with adaptability in mind can better withstand unforeseen challenges (Chang, 2015).

5.2 The Role of AI in Information Resilience

In this digital era, cyberattacks are the most dangerous threats that disrupt national security, hospitals, industries, and several other working systems by hacking into important information. Cyber Attack is not limited to the digital domain; first, they attack digitally, then enter into the physical realm, like the Colonial Pipeline companies attacking the US, and healthcare services attacking in New Zealand. So, a resilient cybersecurity system is very important.

AI can significantly contribute to information resilience by automating threat detection, predicting potential risks, and enabling adaptive security measures. These technologies enhance the agility and responsiveness of information systems (Fiksel, 2015). Advanced analytics tools help organizations to make sense of big data by providing insights into potential risks and vulnerabilities (Tan et al., 2021). Predictive analytics, in particular, aids in foreseeing and mitigating future challenges.

While strides have been made in enhancing information resilience, challenges persist (Morabito, 2015). Moreover, the interconnected nature of global information systems necessitates international collaboration and standardization to address resilience on a broader scale (Molden et al., 2017).

6. Selected Cases

The section will deal with major initiatives, policies related to cybersecurity.

6.1. The UN Resolution on Artificial Intelligence

Recognizing the potential of AI technologies that can facilitate and speed up achieving the 17 Sustainable Development Goals, the UN General Assembly adopted a resolution on the promotion of “safe, secure and trustworthy artificial intelligence (AI) systems that will also benefit sustainable development for all”. In

March 2024, the document was adopted and signed by more than 120 Member States. The document called on all Member States and stakeholders "to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights. The same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems." (Vercelli & United Nations, 2024) The declaration also urged all governments, businesses, civil society, academic institutions, and the media to create and promote frameworks and regulatory measures for the safe, secure, and reliable use of artificial intelligence.

6.2. The United States

The United States President Biden Issued an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence on October 30, 2023. The "Including work that led to voluntary commitments from 15 leading companies to drive safe, secure, and trustworthy development of AI." The primary objective of the U.S. Cybersecurity Strategy is to safeguard the nation's critical infrastructure, protect national security interests, and ensure the resilience of government systems against cyber threats (Nyström et al., 2019).

Government Initiatives: The U.S. government plays an important role in cybersecurity through different agencies like Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and others.

Federal Agencies: The Cybersecurity and Infrastructure Security Agency (CISA) is the leading federal agency for protecting and coordinating cybersecurity in US. The National Institute of Standards and Technology (NIST) develops cybersecurity standards and guidelines. The Department of Homeland Security (DHS) and Department of Defences (DOD) are also playing major roles in cybersecurity.

Executive Orders: These orders may be targeted on specific areas such as protecting critical infrastructure, improving federal cybersecurity or enhancing information sharing between government organization and private sector agencies.

The National Institute of Standards and Technology (NIST) and Defences Advanced Research Projects Agency (DARPA) play an important role in advancing AI technologies and addressing cybersecurity challenges (General Assembly Adopts Landmark Resolution on Artificial Intelligence, 2024).

6.3. The Bletchley Declaration

The Bletchley Declaration was adopted by several countries attending the AI Safety Summit, during 1-2 November 2023, held at Bletchley Park, England (House, 2023). Representatives from 28 major countries, including the United States, China, India, and the European Union, came together to sign this ground-breaking declaration (Roesener et al., 2014).

The declaration highlights the necessity of worldwide cooperation to handle the inherent global nature of AI-related risks. It calls for collaboration among all stakeholders, including companies, civil society, and

academia. The declaration also says the establishment of a regular AI Safety Summit to facilitate dialogue and collaboration among various stakeholders on frontier AI safety and security (Street, 2025; The Bletchley Declaration – Everything AI, n.d.).

6.4 Budapest Convention on Cybercrime:

The first international convention on cybercrime (also known as the Convention on Cybercrime) was held in 2001 and came into force in 2004. The convention discussed several issues, including copyright infringement, child pornography, computer-related crime, and violations of cybersecurity. For the first time, cybercrime became a global agenda because of the extensive development of the internet and web technologies. The convention addresses the major issues like illegal use of computer data, data interference, and misuse of devices, copyright infringement, and computer-related fraud.

The Budapest Convention provides standardized guidelines on the preservation, collection, and use of digital data. The Budapest Convention was a major step because it created a platform for countries to fight cybercrime with the help of Budapest's technical expertise (Makam, 2023; Convention on Cybercrime, 2001).

6.5 International Telecommunication Union (ITU):

ITU developed the 'Global Cybersecurity Agenda' (GCA) to build trust and security in ICT. CGA stands on five pillars: legal measures, technical and procedural measures, organisational structures, capacity building, and International corporations. ITU published the global cyber index to highlight the major problems of member countries and provide suggestions for the improvement of cybersecurity. ITU developed three programmes based on ICT's 'Global Cyber Security Index', 'National Cyber Security strategies', and the 'national CRT programmes'. Above all, ITU supports its member countries to build national cybersecurity strategies that are crucial for resilient digital growth [28].

It powers numerous programmes, including the Global Cybersecurity Index (GCI), national Computer Incident Response Teams (CIRTs), Cyber Drills, Child Online Protection (COP), and strategic partnerships like International Multilateral Partnership against Cyber Threats (IMPACT) (Matamis, 2024).

6.6. India

India advocates for a global framework to expand the use of "ethical" AI tools, demonstrating a commitment to responsible AI usage. India expresses interest in establishing regulatory bodies at both domestic and international levels to ensure responsible AI use. The Digital India Act, 2023, which is yet to be implemented, is expected to introduce specific regulations for online intermediaries, including AI-based platforms (Digital India Act, 2023).

India National Cyber Security Policy 2013

The National Cyber Security Policy 2013 established the National Critical Information Infrastructure Protection Centre (NCIIPC) as a significant step towards enhancing the protection and resilience of the nation's critical

information infrastructure. The NCIIPC operates around the clock (24/7) and is responsible for safeguarding critical information infrastructure (CII) in India. The National Cyber Security Policy 2013 indeed emphasized the establishment and operation of a 24x7 National Level Computer Emergency Response Team (CERT-In). CERT-In serves as the nodal agency for coordinating all efforts related to cybersecurity emergency response and crisis management in India. It operates around the clock to respond promptly to cybersecurity incidents and crises. This Policy aims to ensure a comprehensive and coordinated effort to enhance cybersecurity across various levels of governance and operation, acknowledging the diverse challenges posed by cyberspace security (National Cyber Security Policy, 2013)

6.7. China

The Chinese government has implemented several regulations and laws aimed at enhancing cybersecurity within its territory. One of the most notable is the Cybersecurity Law, which came into effect in 2017. China's internet security system is often referred to as the 'Great Firewall.' These systems monitor the internet traffic of China (China's Data Governance and Cybersecurity Regime, n.d.).

Cybersecurity Laws (CSL)

The CSL is one of the most comprehensive cybersecurity laws globally. It introduced in 2017. It imposes obligations on network operators to safeguard data, report security incidents, undergo security assessments, and store data within Chinese territory.

The key provisions of the law include requirements for the protection of personal information, Critical Information Infrastructure (CII) security, and the conduct of security reviews for network products and services.

National Intelligence Law

Implemented in 2017, the National Intelligence Law authorizes Chinese intelligence agencies to compel organizations and individuals to cooperate with intelligence work, including access to data and network facilities. While not explicitly focused on cybersecurity, the above-stated law has implications for data governance and cybersecurity by granting authorities broad powers to access and monitor information (PricewaterhouseCoopers, n.d).

Data Security Law (DSL)

Enacted in 2021 and set to come into effect in September 2021, the DSL focuses specifically on data security and aims to regulate the collection, storage, processing, transmission, and use of data within China. Additionally, the DSL introduces a data classification system and establishes mechanisms for cross-border data transfers, with a requirement for security assessments and approval by authorities for certain types of data (Data Security Law of the People's Republic of China, n.d.).

6.8 Singapore

Singapore is ranked 2nd in digital and technological competitiveness in Asia. It is the top intellectual protector country in Asia and second globally. Singapore's cybersecurity work started in 2005, and in 2015, it established the Cybersecurity Agency Singapore (CAS). Recently, the Singapore government published the "Singapore Cybersecurity Strategies 2021"(Loong et al., 2021)

The Singapore government has built a national internet infrastructure, a software as a service platform (SaaS), domain name security extension that helps to prevent cyber threats in the country. Cybersecurity agencies are deploying AI models on their security systems to build a resilient security wall. Singapore developed cybersecurity products that are popularised globally, like the cybersecurity levelling schema on their smart devices. The Singapore government helps with cybersecurity research projects, research on real products, and building cybersecurity skills. A secure, open, resilient cybersecurity helps economic growth and builds a smart nation (Singapore - Information and Telecommunications Technology, 2024; Vu, 2016).

6.9. Case of Microsoft Security

The progress of technology creates strong cybersecurity and safety precautions. In Microsoft's security, there are the following components:

Cybersecurity Policy Framework: Microsoft offers a practical guide for the development of national cybersecurity policies.

Cloud Policy Framework: Microsoft advocates for a secure and resilient cloud computing environment, benefiting government productivity and communication.

Identity Protection: As part of its security strategy overhaul, Microsoft focuses on enhancing identity protection across its products (Microsoft Security. (n.d.)

Microsoft adopted the following principles for influencing Microsoft's policies and initiatives to reduce the risks related to nation-state advanced persistent threats (APTs), advanced persistent manipulators (APMs), and cybercrime syndicates using AI tools and APIs. These principles include identifying and combating malevolent threats, Notification of more AI service suppliers, Collaboration with other stakeholders, and Transparency.

Microsoft offers information concerning the kind and scope of threat actors' usage of AI detected within their systems, as well as the necessary countermeasures (Microsoft Security Blog, 2001).

6.10. Case of Apple's Security

Apple is widely recognised for its strong cybersecurity architecture, which is essential to protect both its devices and user data. Devices such as iPhones, iPads, and Macs incorporate a Secure Enclave, a dedicated security coprocessor that manages cryptographic operations, including those for Touch ID and Face ID.

This hardware ensures that sensitive biometric data is stored in isolation, keeping it protected from unauthorized access (Apple Platform Security, n.d).

Apple's operating systems—iOS and macOS—offer multiple security layers designed to resist various cyber threats. These mechanisms work collectively to prevent system compromise and reduce vulnerability exposure (Apple Security Releases - Apple Support, 2025).

WhatsApp has implemented an Auditable Key Directory (AKD)—a KT-based system that improves performance and scalability by batching key updates. AKD represents a modern, scalable approach to public key verification in messaging apps (Stebila & Apple Inc., 2024)

6.11. Open AI Security

OpenAI implements comprehensive encryption strategies to secure sensitive data both at rest and in transit. Communications between systems are encrypted using secure protocols such as SSL/TLS, while data stored on OpenAI's infrastructure is likely protected with strong cryptographic algorithms to prevent unauthorized access and maintain data confidentiality (Cybersecurity Grant Program Application, n.d.).

To further safeguard its infrastructure, OpenAI presumably enforces strict access controls. These include the use of multi-factor authentication (MFA), role-based access control (RBAC), and routine access audits. These measures ensure that only personnel with a legitimate need can access specific systems or data, minimising the risk of internal or external breaches (Open AI Security Overview, n.d). OpenAI focuses on the areas of empowering defenders, measuring capabilities, and enhancing discourse.

7. Concluding Remarks

Cybersecurity frameworks emphasise proactive, AI-powered threat detection systems integrated with real-time response mechanisms. Building on international collaborations such as the 'Bletchley Declaration', 'UN Resolutions', and frameworks like the 'Budapest Convention', nations should prioritise harmonised global standards, regular AI safety summits, and data-sharing agreements to mitigate transnational cyber threats. Institutions should adopt AI-driven systems that ensure information resilience, particularly by automating risk assessments, forecasting threats through predictive analytics, and reinforcing adaptive and encrypted infrastructures.

In the future, advanced implementations may include federated learning for privacy-preserving data analysis, quantum-resilient encryption to counter next-generation threats, and AI auditing frameworks to enhance transparency and trust. Moreover, establishing independent global regulatory bodies, as suggested by countries like India, and fostering public-private partnerships will be crucial to support research, innovation, and ethical AI deployment. A resilient digital ecosystem must not only rely on technological measures but also embed legal, organisational, and human-centred safeguards to future-proof the integrity and security of global information systems.

The increasing cyberattacks in various sectors are a matter of global concern. International agencies like the United Nations, many governments around the world, as well as big firms, are using AI technologies to improve security and maintain stability in information resilience.

From a Library and Information Science (LIS) perspective, this paradigm shift in global cyber security scenario is especially significant. Libraries are no longer passive repositories of knowledge but critical nodes in the digital ecosystem. In the present information society, safeguarding of user data, ensuring privacy, and promoting equitable access are central responsibilities of libraries globally. Digital libraries and institutional repositories face rising threats such as data breaches, ransomware, and misinformation campaigns. Hence, cybersecurity is a key component of modern library management.

Implementations are expected to include federated learning for privacy-preserving data analysis**,** quantum-resilient encryption to counter next-generation threats, and AI auditing frameworks to improve transparency and trust. For libraries, such tools can enhance the security of digital archives, open access databases, and library management systems (ILMS/Koha).

Establishing independent global regulatory bodies, as proposed by countries such as India, alongside fostering public–private partnerships, will be essential to support research, innovation, and the ethical deployment of AI. Libraries, through consortia such as IFLA, ALA, and national library networks, can act as bridges between global standards and local implementation, ensuring that cybersecurity measures align with principles of intellectual freedom and equitable access.

As there are diverse ranges of cyber threat actors, it is quite impossible for any single entity to manage these risks independently. Hence, a unified global approach is must. Emerging cyber-collaborative systems, which integrate physical infrastructure with AI technologies to enable secure machine-to-machine communication, may prove transformative in preventing disruptions, strengthening defences, and building AI-powered, information-resilient cyber ecosystems. In this environment, libraries can serve as community hubs for digital resilience, offering not only secure access to knowledge but also fostering digital ethics, data protection practices, and human-centred safeguards that reinforce global cybersecurity efforts.

8. Acknowledgement

We acknowledge that a pre-version of this manuscript was uploaded to the preprint server (Preprints.org). Mandal, S., & Patra, S. K. (2024). Artificial Intelligence and Cybersecurity: A Global Scenario. Preprints. https://doi.org/10.20944/preprints202405.0415.v1

9. References

1. Alnaffar, A. (2024). Cybersecurity Resilience awareness in the era of AI. International Journal of Science and Research (IJSR), 13(3), 244–245. https://doi.org/10.21275/sr24305145928

2. Apple Platform Security. (n.d.). Apple Support. https://support.apple.com/en-in/guide/security/welcome/web

3. Apple security releases - Apple Support. (2025, June 12). Apple Support. https://support.apple.com/en-us/100100

4. Black, J. (2023). Past, present and tackling the future of artificial intelligence (AI) in education: maintaining agency and establishing AI laws. Open Journal of Social Sciences, 11(07), 442–464. https://doi.org/10.4236/jss.2023.117031

5. Chang, V. (2015). Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, 65–82. https://doi.org/10.1016/j.adhoc.2015.07.012

6. China's Data Governance and Cybersecurity Regime. (n.d.). http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209.

7. Convention on Cybercrime. (2001). https://rm.coe.int/1680081561.

8. CSRC Content Editor. (n.d.). resilience - Glossary | CSRC. https://csrc.nist.gov/glossary/term/resilience

9. Cyber Security. (n.d.). https://www.itgovernance.co.uk/what-is-cybersecurity

10. Cybersecurity Grant Program application. (n.d.). https://openai.com/form/cybersecurity-grant-program/.

11. Data Security Law of the People's Republic of China. (n.d.). http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html

12. Digital India Dialogues. (2023). Digital India Act, 2023. In Digital India Dialogues. https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

13. Fiksel, J. (2015). Resilient by design. In Island Press/Center for Resource Economics eBooks. https://doi.org/10.5822/978-1-61091-588-5

14. General Assembly adopts landmark resolution on artificial intelligence. (2024, August 30). UN News. https://news.un.org/en/story/2024/03/1147831

15. Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I., & Ramkumar, P. N. (2020). Machine learning and Artificial intelligence: definitions, applications, and future directions. Current Reviews in Musculoskeletal Medicine, 13(1), 69–76. https://doi.org/10.1007/s12178-020-09600-8

16. House, W. (2023, November 3). WHAT THEY ARE SAYING: President Biden issues Executive Order on Safe, Secure, and trustworthy artificial intelligence. The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/31/what-they-are-saying-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

17. Hüsch, P., Sullivan, J., Royal United Services Institute for Defence and Security Studies, & (ISC)². (2023a). Global Approaches to Cyber Policy, Legislation and Regulation: A Comparative Overview. In

Royal United Services Institute for Defence and Security Studies, RUSI Special Resources. https://static.rusi.org/rusi-global-approaches-to-cyber-special-resource_0.pdf

18. Hüsch, P., Sullivan, J., Royal United Services Institute for Defence and Security Studies, & (ISC)². (2023b). Global Approaches to Cyber Policy, Legislation and Regulation: A Comparative Overview. In Royal United Services Institute for Defence and Security Studies, RUSI Special Resources. https://static.rusi.org/rusi-global-approaches-to-cyber-special-resource_0.pdf

19. IT Governance Ltd. (2013). CYBERSECURITY: a CRITICAL BUSINESS RISK [Green Paper]. In IT Governance Green Paper (pp. 2–4). https://www.itgovernance.co.uk/download/Cybersecurity-v4.pdf

20. Jobs, S. (2010). A day in the life of your data [Journal-article]. All Things Digital Conference, 3. https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

21. Kassim, S. R. B. M., Li, S., & Arief, B. (2023). The use of public data and free tools in National CSIRTs' operational practices: A systematic literature review. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.07988

22. Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial intelligence and machine learning. Electronic Markets, 32(4), 2235–2244. https://doi.org/10.1007/s12525-022-00598-0

23. Laksito, J., Pratiwi, B., & Ariani, W. (2025). Harmonizing Data Privacy Frameworks in Artificial Intelligence: Comparative Insights from Asia and Europe. Perkara., 2(4), 579–588. https://doi.org/10.51903/perkara.v2i4.2229

24. Landoll, D. (2021). The Security Risk Assessment Handbook. https://doi.org/10.1201/9781003090441

25. Linkov, I., & Kott, A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In Springer eBooks (pp. 1–25). https://doi.org/10.1007/978-3-319-77492-3_1

26. Loong, H., Cyber Security Agency of Singapore, The Singapore Cyber Security Inter Association, The Cyber Security Awareness Alliance, The Infocomm Media Development Authority, The Ministry of Communications and Information, The Ministry of Defence, The Ministry of Home Affairs, The Personal Data Protection Commission, The Singapore Police Force, & The Smart Nation and Digital Government Group. (2021). The Singapore Cybersecurity Strategy 2021. https://ccdcoe.org/uploads/2018/10/Singapore_Cybersecurity_Strategy_2021.pdf

27. Lourens, M., Dabral, A. P., Gangodkar, D., Rathour, N., Tida, C. N., & Chadha, A. (2022). Integration of AI with the Cybersecurity: A detailed systematic review with the practical issues and challenges. International Conference on Contemporary Computing and Informatics, 1290–1295. https://doi.org/10.1109/ic3i56241.2022.10073040

28. Makam, G. (2023). India's Evidence Act and the case for joining the Budapest Convention: A comprehensive analysis of cyber evidence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4495729

29. Matamis, J. (2024). The International Telecommunications Union (ITU) and cyber accountability. Stimson Center. https://www.stimson.org/2024/the-international-telecommunications-union-itu-and-cyber-accountability/

30. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine, 27(4), 12. https://doi.org/10.1609/aimag.v27i4.1904

31. Michalski, R., Carbonell, J., & Mitchell, T. (2013). Machine learning: An Artificial Intelligence Approach. Springer Science & Business Media.

32. Microsoft Security Blog. (2001, May 29). Threat intelligence | Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/

33. Molden, D., Sharma, E., Shrestha, A. B., Chettri, N., Pradhan, N. S., & Kotru, R. (2017). Advancing regional and transboundary cooperation in the Conflict-Prone Hindu Kush–Himalaya. Mountain Research and Development, 37(4), 502–508. https://doi.org/10.1659/mrd-journal-d-17-00108.1

34. Morabito, V. (2015). Big data and Analytics. In Springer eBooks. https://doi.org/10.1007/978-3-319-10665-6

35. National Cyber Security Policy -2013. (2012). In https://www.meity.gov.in/.

36. Nyström, M., Jouffray, J., Norström, A. V., Crona, B., Jørgensen, P. S., Carpenter, S. R., Bodin, Ö., Galaz, V., & Folke, C. (2019). Anatomy and resilience of the global production ecosystem. Nature, 575(7781), 98–108. https://doi.org/10.1038/s41586-019-1712-3

37. Open AI Security Overview. (n.d.). https://openai.com/security-and-privacy/.

38. PricewaterhouseCoopers. (n.d.). A comparison of cybersecurity regulations: China. PwC. https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html

39. Roesener, A. G., PhD, Bottolfson, C., & Fernandez, G. (2014). Policy for US cybersecurity. In Air Force Research Institute (AFRI), Air & Space Power Journal. https://apps.dtic.mil/sti/pdfs/ADA617837.pdf

40. Singapore - Information and Telecommunications Technology. (2024, January 5). International Trade Administration | Trade.gov. https://www.trade.gov/country-commercial-guides/singapore-information-and-telecommunications-technology

41. Sontan, N. a. D., & Samuel, N. S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607

42. Stebila, D. & Apple Inc. (2024). Security analysis of the iMessage PQ3 protocol [Journal-article]. https://security.apple.com/assets/files/Security_analysis_of_the_iMessage_PQ3_protocol_Stebila.pdf

43. Street, P. M. O. 1. D. (2025, February 13). The Bletchley Declaration by countries attending the AI Safety Summit, 1-2 November 2023. GOV.UK. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

44. Tan, L., Yu, K., Ming, F., Cheng, X., & Srivastava, G. (2021). Secure and Resilient Artificial Intelligence of Things: A HoneyNet approach for threat detection and situational awareness. IEEE Consumer Electronics Magazine, 11(3), 69–78. https://doi.org/10.1109/mce.2021.3081874

45. The Bletchley Declaration – everything AI. (n.d.). https://thebletchleydeclaration.com/

46. Van Den Adel, M. J., De Vries, T. A., & Van Donk, D. P. (2021). Resilience in interorganizational networks: dealing with day-to-day disruptions in critical infrastructures. Supply Chain Management an International Journal, 27(7), 64–78. https://doi.org/10.1108/scm-03-2021-0136

47. Vercelli, A. & United Nations. (2024). United Nations, artificial intelligences and regulations: analysis of the General Assembly AI Resolutions and the Final Report of the Advisory Body on AI. In INHUS – CONICET, Grupo CITEUS, Facultad De Humanidades / Universidad Nacional De Mar Del Plata [Journal-article]. https://ceur-ws.org/Vol-3881/paper11.pdf

48. Vu, C. (2016). CYBER SECURITY IN SINGAPORE. https://www.rsis.edu.sg/wp-content/uploads/2016/12/PR170217_Cybersecurity-in-Singapore.pdf

49. What is Cybersecurity? Key Concepts Explained | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity

50. Wikipedia contributors. (2024, June 21). International Multilateral Partnership against Cyber Threats. Wikipedia. https://en.wikipedia.org/wiki/International_Multilateral_Partnership_Against_Cyber_Threats

About Authors

Subhadip Mandal, Library Professional Trainee, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh
Email: subhadipmandal399@gmail.com
ORCID: https://orcid.org/0009-0007-9814-9354

Kanu Chakraborty, Assistant Librarian, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh
Email: kchakraborty.lib@iitbhu.ac.in
ORCID: https://orcid.org/0000-0003-3911-2176

Dr Swapan Kumar Patra, Assistant Professor, Department of Library & Information Science, Sidho-Kanho-Birsha University, Purulia, West Bengal
Email: skpatra@gmail.com & skpatra@skbu.ac.in
ORCID: https://orcid.org/0000-0002-0825-7973

Dr Navin Upadhyay, Deputy Librarian, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh
Email: nupadhyay.lib@iitbhu.ac.in
ORCID: https://orcid.org/0000-0002-7956-7936

Anisha Kumari, Library Attendant, Rajarshi Janak Central library, CUSB, GAYA, Bihar
Email:dubeyanisha603@gmail.com
ORCID: https://orcid.org/0009-0007-8232-4285