Article

Not peer-reviewed version

Artificial Intelligence and Cybersecurity: A Global Scenario

Subhadip Mandal and Swapan Kumar Patra [*]

Posted Date: 8 May 2024

doi: 10.20944/preprints202405.0415.v1

Keywords: artificial intelligence; machine learning; information resilience; robustness; data bias

Article

Artificial Intelligence and Cybersecurity: A Global Scenario

Subhadip Mandal and Swapan Kumar Patra *

Sidho-Kanho-Birsha University, India
* Correspondence: skpatra@gmail.com

Abstract: Introduction: Artificial Intelligence (AI) tools and techniques are comparatively recent advances of present-day globalized world. With their easy availability and friendly user interface AI has affected in every sphere of human being. These tools are increasingly becoming popular because of numerous benefits occurred to the society in many ways. However, there are not only the positive side of these technologies, but also many negative sides. Along with the development and adoption of AI, cyber-attacks are increased and disrupting the information system. Threat actors may misuse artificial intelligence. Hence, these tool designers are working and applying the ability of generative AI can tip the scales in cybersecurity. So, in the age of AI, there is always a tension between the cyber attackers and the defenders to make balanced information system. It is a general rule that defenders must be well in advance in their favor and keep ahead of adversaries. The United National and several governments for example the US, UK, and the big AI giants like Microsoft along with OpenAI, are working on emerging cyberattacks. They are focusing on identifying the unusual activities associated with both known and unknown threat actors. **Purpose:** The purpose of this paper is to investigate cybersecurity issues and subsequent policies adopted by various agencies. This paper is a review of the policy statements adopted by selected governments and the subsequent policy measures taken by the big multinational corporation. This study will do a critical analysis on "The Bletchley Declaration," President Biden's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence and the strategies adopted by the big Information Technology (IT) firms like Apple, Microsoft, and Open AI. **Design/ methodology/ Approach:** For this study, we have investigated the recently adopted policies of the United Nations, China, India. US and UK governments. We have also analysed the issues dealt by the two big technology giants Microsoft and OpenAI. **Originality:** The paper has done a critical analysis of both government and corporate policies to deal with the cybersecurity issues. Globally, there is an increasing trend of increasing adoption of AI in every sphere of human life. With this growing use there is a major apprehension of safety, security, integrity, and robustness of information system. So, it is a matter if concern how the information system deals with this issue. In this context, the paper is going to shed light on these pressing challenges from the available literature. **Conclusion:** Information systems often face challenges related to the issues of data quality, robustness, and security. Although the recent advances of AI and other related technologies, it is becoming easier to build quite resilient information system. However, information system, can compromise their performance and reliability due to the security issues. This research paper explores the concept of information resilience in ML and AI systems, focusing on strategies to enhance their ability to withstand uncertainties, adversarial attacks, and data perturbations.

Keywords: Artificial Intelligence; Machine Learning; information resilience; robustness; data bias

1. Introduction

The term "*Artificial Intelligence*" (AI) was coined by '*Minsky and McCarthy*' [1] in 1956 to denote the theory of human intelligence being exhibited by machines [2]. 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. Machine learning (ML) and AI systems are all pervasive in present day globalized world. AI influence in every domain, ranging from healthcare to finance, and from autonomous vehicles to cybersecurity [3]. However, these systems often face challenges related to data quality, robustness, and security. These issues altogether can compromise their performance and reliability.

This research paper explores the concept of information resilience in ML and AI systems, focusing on strategies to enhance their ability to withstand uncertainties, adversarial attacks, and data perturbations. While doing so, the paper is going to review approaches taken by the government agencies and the strategies taken by several big multinational firms. This paper examines these policies and techniques to improve the resilience of these systems, thereby ensuring their reliability and trustworthiness in real-world applications.

2. Artificial Intelligence

"AI leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind. AI lists theorem proving, game playing, pattern recognition, problem solving, adaptive programming, decisions making, music composition by computer, learning networks, natural language data processing and verbal and concept learning as suitable topics." (ACM Curriculum committee) [4].

The first computational models intended to imitate human intellect appeared in the middle of the 20th century, when artificial intelligence (AI) first emerged. However, it is the advent of sophisticated algorithms, coupled with the exponential growth in computational power and data availability, that has propelled ML and AI to the forefront of technological innovation in recent years [5].

AI and its subfield ML gained significant traction in current years due to their ability to handle massive volume of data. These systems can extract meaningful insights quickly, and can make autonomous decisions without explicit programming. The significance of ML and AI systems lies in their potential to revolutionize numerous aspects of human endeavour, ranging from improving efficiency and productivity to enhance decision-making and problem-solving. Some key areas where ML and AI are making a profound impact include healthcare, finance, autonomous systems, cybersecurity etc [6].

3. Information Resilience

Information resilience means the power of a system to maintain its functionality, integrity, and performance in the face of disturbances, uncertainties, adversarial attacks, and changes in the environment or operating conditions. National Institute of Standard and Technology (NIST), US Department of Commerce defines Information Resilience as *"The ability to maintain required capability in the face of adversity"* [7]. *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 maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs"* [8].

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.

3.1. Information Resilience and Cybersecurity

As discussed earlier, information resilience refers to the ability of systems, organizations, and individuals to withstand and recover from disruptions, ensuring the availability, integrity, and confidentiality of information. 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 & Machine Learning on in Cybersecurity.

"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" [9]. It encompasses various measures to defend against cyber threats, including:

Network Security: Securing networks to prevent unauthorized access and ensure data integrity

Data Security: Safeguarding sensitive information through encryption, access controls, and data loss prevention.

Endpoint Security: Protecting individual devices like computers, smartphones, and IoT devices from malware and other cyber threats.

AI and ML algorithms can analyze patterns in data to identify abnormal behavior that can point to a security risk. This is particularly useful for detecting unusual patterns in network traffic, user behavior, or system activities. Machine Learning models can forecast possible security threats based on historical data, helping organizations to take proactive measures. 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. Moreover, AI can contribute to the improvement of encryption algorithms and techniques, making it more challenging for unauthorized entities to access sensitive information. Machine learning models can be designed to process data while preserving individual privacy, using techniques like federated learning or homomorphic encryption.

3.2. Strategies for Information Resilience

Organizations carry out thorough risk assessments to find possible weak points and threats [10]. This involves understanding the threat landscape, assessing potential impacts, and prioritizing risk mitigation strategies.

Robust cybersecurity practices form a crucial component of information resilience [11]. Implementation of firewalls, intrusion detection systems, and encryption technologies safeguards information assets from unauthorized access and cyber threats.

Business continuity planning ensures that organizations can maintain critical functions during disruptions [12]. This involves creating contingency plans, establishing backup systems, and conducting regular drills to prepare for various scenarios.

Regular data backups and efficient recovery mechanisms safeguard against data loss [13]. This includes automated backup solutions, off-site storage, and streamlined recovery processes.

Information systems designed with adaptability in mind can better withstand unforeseen challenges [14]. Cloud computing, decentralized architectures, and scalable solutions contribute to the adaptability of information infrastructure.

3.3. The Role of Technology in Information Resilience

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 [15].

Advanced analytics tools help organizations make sense of vast amounts of data, providing insights into potential risks and vulnerabilities [16]. Predictive analytics, in particular, aids in foreseeing and mitigating future challenges.

While strides have been made in enhancing information resilience, challenges persist [17]. Rapid technological advancements, evolving cyber threats, and the increasing volume of data pose ongoing challenges. Moreover, the interconnected nature of global information systems necessitates international collaboration and standardization to address resilience on a broader scale [18].

4. Selected Cases

Various government and big multinational firms have adopted policies, guidelines and issued statements to mitigate cyberattacks for an information resilient system. The following section will deal with a few major initiatives, policies related to cybersecurity issues:

4.1. The UN Resolution on Artificial Intelligence

Recognising the potential of AI technologies 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."* 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. [19]

4.2. The United States

In the United States President Biden Issues 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.*" [20]

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.

Government Initiatives: The U.S. government plays a significant role in cybersecurity through various agencies such as the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and others. These agencies work to protect critical infrastructure, investigate cybercrimes, and share threat intelligence.

Executive Orders: The President can issue executive orders to establish cybersecurity policies and directives. These orders may focus on specific areas such as improving federal cybersecurity, protecting critical infrastructure, or enhancing information sharing between government and private sector entities.

Federal Agencies: Various federal agencies have roles and responsibilities related to cybersecurity. For instance, the Cybersecurity and Infrastructure Security Agency (CISA) is the lead federal agency for protecting critical infrastructure and coordinating cybersecurity efforts. The National Institute of Standards and Technology (NIST) develops cybersecurity standards and guidelines, while the Department of Homeland Security (DHS) and the Department of Defence (DoD) are also heavily involved in cybersecurity efforts [21].

Public-Private Partnerships: Collaboration, the public and commercial sectors can successfully combat cybersecurity risks. Initiatives like the Information Sharing and Analysis Centers (ISACs) facilitate the sharing of threat intelligence and best practices among different industries.

The U.S. invests in research and development (R&D) initiatives aimed at advancing AI technologies for cybersecurity. This includes funding for academic research, supporting industry innovation, and collaboration with the private actors to develop AI-driven cybersecurity solutions.

Initiatives such as the National Institute of Standards and Technology (NIST) and the Defence Advanced Research Projects Agency (DARPA) play a significant role in advancing AI capabilities and addressing cybersecurity challenges [22].

4.3. The Bletchley Declaration

The Bletchley Declaration was adopted by several countries attending the AI Safety Summit, during 1-2 November 2023 [23]. The Artificial Intelligence Safety Summit held at Bletchley Park, England. Representatives from 28 major countries, including the United States, China, India, and the European Union, came together to sign this ground breaking declaration [24]. This declaration represents a high-level political consensus among major AI players worldwide. The declaration represents a critical turning point in the global strategy to address the issues raised by cutting-edge AI technologies. It recognizes the potential advantages of AI for improving human welfare. Simultaneously, it recognizes the risks posed by AI, particularly frontier AI. Frontier AI is the term for extremely powerful generative AI models that can generate realistic outputs (text, graphics, audio, or video) whenever needed. The conference has observed the many positive as well as negative sides of the AI.

Recommendations of Bletchley Park Declaration

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 standing of a regular AI Safety Summit to facilitate dialogue and collaboration among various stakeholders on frontier AI safety and security. In summary, the Bletchley Declaration aims to harness the positive potential of AI while addressing risks, ensuring that AI benefits everyone and is used responsibly.

4.4. India

India has shifted from a position of not considering AI regulation to actively formulating regulations based on a risk-based, user-harm approach. India advocates for a global framework to expand the use of "ethical" AI tools, demonstrating 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 issue-specific regulations for online intermediaries, including AI-based platforms [25].

India National cyber security policy 2013

The National Cyber Security Policy 2013 established the National Critical Information Infrastructure Protection Centre (NCIIPC) was a significant step towards enhancing the protection and resilience of the nation's critical information infrastructure. The NCIIPC operates round the clock (24x7) and is tasked with the responsibility of safeguarding critical information infrastructure (CII) in India. It monitors, detects, and responds to cyber threats targeting critical sectors such as energy, finance, transportation, telecommunications, and government services.

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 cyber security emergency response and crisis management in India. It serves as the central coordinating authority for all cyber security-related activities within the country. It operates round the clock to respond promptly to cyber security incidents and crises. It provides technical assistance and guidance to organizations facing cyber threats or attacks.

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 [26].

4.5. China

Cybersecurity in China has been a significant focus for the government due to the country's growing reliance on technology and the internet. The Chinese government has implemented various regulations and laws aimed at enhancing cybersecurity within the country. One of the most notable is the Cybersecurity Law, which came into effect in 2017. This law regulates various aspects of cybersecurity, including data protection, critical information infrastructure security, and cybersecurity reviews for network products and services. China operates one of the most sophisticated internet censorship systems in the world. China's internet security system often referred to as the 'Great Firewall.' This system controls and monitors internet traffic entering and leaving China. The system blocks access to certain websites and content deemed politically sensitive or harmful to national interest [27].

Cybersecurity Law (CSL) in China

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

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

The CSL also grants broad powers to investigate cybersecurity incidents, enforce compliance, and punish non-compliant entities to the Chinese government.

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 [28].

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. The DSL requires data handlers to secure sensitive and personal data, get permission before processing it, and put security measures in place to stop illegal access or disclosure.

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 [29].

4.6. Case of Microsoft Security

The progress of technology creates Strong cybersecurity and safety precautions. In the 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 [30].

Microsoft adopted 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. Microsoft's cybersecurity policy involves partnering with governments and policymakers globally to address cybersecurity challenges. These principles include:

identifying and combating malevolent threat actors use: If Microsoft AI application programming interfaces (APIs), services, or systems are used by any nation-state APT or APM, cybercrime syndicates monitor, or any other identified malicious threat actor, Microsoft will take appropriate action to interrupt their activity. This could entail stopping services, restricting access to resources, or disabling the used accounts.

- Notification of more AI service suppliers: Microsoft will swiftly notify other service providers and disclose pertinent data when they discover a threat actor using their AI, AI

APIs, services, and/or systems. This lets the service provider follow their own policies and independently confirm Microsoft's findings.

- Collaboration with other stakeholders: Microsoft identify threat actors using AI. Its guiding philosophy is to work with other interested parties to regularly exchange information on threat actors. In this way Microsoft, encourage, coordinate, dependable, and effective responses to threats for an information resilient ecosystem.

Transparency: To maintain the transparency in the whole ecosystem, Microsoft decide to notify all stakeholders and the public about actions taken in accordance with these threat actors. As part of our continuing efforts to improve responsible use of AI, it offers information concerning the kind and scope of threat actors' usage of AI detected within their systems as well as the necessary countermeasures [31].

4.7. Case of Apple's Security

Apple is widely recognized for its robust cybersecurity measures. It is integral to maintain the security and privacy of its products and services. Apple's devices, such as iPhones, iPads, and Macs, incorporate a "*Secure Enclave*." It is dedicated coprocessor responsible for handling cryptographic operations related to Touch ID, Face ID, and other security-sensitive tasks. The '*Secure Enclave'* ensures that sensitive data like biometric information remains protected and inaccessible to unauthorized parties. Mac computers equipped with Apple's T2 Security Chip benefit from hardware-based encryption, secure boot capabilities, and storage of cryptographic keys. This chip enhances the security of the device by verifying the integrity of the boot process and providing hardware-based encryption for data storage.

Apple's operating systems, iOS, and macOS, include multiple layers of security mechanisms to protect against various threats. These include sandboxing of applications, data encryption, secure boot processes, code signing, and runtime protections such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP). Additionally, Apple provides regular security updates and patches to address known vulnerabilities and mitigate emerging threats.

Privacy is a fundamental aspect of Apple's cybersecurity strategy. The company minimizes the collection of users' data, provides transparency about how data is used, and gives users control over their personal information. Features such as App Tracking Transparency, which allows users to block cross-app tracking, demonstrate Apple's commitment to protecting user.

Apple's iMessage debuted in 2011 became the first messaging app that was made available to the public to offer secure end-to-end encryption by default. End-to-end encryption is a feature of iMessage that makes sure that only the sender and recipient may read message. Every device connected to a user's iMessage account creates a unique set of encryption keys to provide this robust security feature, and the private keys are never exported to any other system. iMessage Contact Key Verification employs Key Transparency (KT) as a technique. KT is an extension of Certificate Transparency, but it makes use of a verifiable log-backed map data structure that can be checked for consistency over time and offer cryptographic proofs of inclusion. Better user privacy and increased scalability are made possible by these attributes. Recently, WhatsApp made significant progress in this area by being the first to deploy Auditable Key Directory (AKD), a KT system for messaging that greatly improves the scalability of the relevant data structures by batching map revisions as the key directory service inserts identifiers and keys [32]. The Security Research Device (SRD), do iOS security research without disabling the device's security measures. It is essentially a special feature of iPhone

4.8. Case of Open AI Security

OpenAI extensively uses encryption mechanism to protect sensitive data both at rest and in data transit. This includes encryption protocols such as SSL/TLS for communication between servers and encryption of stored data using strong cryptographic algorithms.

It is probable that OpenAI utilizes stringent access restrictions to grant authorized workers exclusive access to its systems and data. To make sure that only individuals who require access can receive it, this involves putting multi-factor authentication (MFA), role-based access control (RBCA), and frequent access reviews into place.

OpenAI's cybersecurity grant program has project ideas such as: By applying AI and coordinating like-minded people who are working for our collective safety, we hope to shift the power dynamics of cybersecurity in partnership with defenders throughout the world. Through the following issues OpenAI is likely to coordinate the cyber security issues by following addressing the following issues: Empower defenders; Capabilities measurement; Enhance discourse [33]

5. Concluding Remarks

Cybersecurity is an important issue in present day globalized world. The increasing cyber-attack in various sectors is a matter of global concern. International agencies like the United Nations, many governments around the world as well as big firms are using digital technologies to improve the security and maintain stability in information resilience. This can be done by adopting suitable policies, and collaborative efforts from various stakeholders by developing more sustainable products. Because of various types of cyber threat actors, it is perhaps impossible for an entity to deal with these issues. Hence all stake holders call for a unified approach to deal with the cybersecurity issues. Cyber collaborative systems are a combination of physical and digital technology that allows machines to communicate and work together. This might improve cybersecurity, prevent unexpected disruption in information system and can build an information resilient system.

References

1. 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), 12-12.
2. Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. *Current reviews in musculoskeletal medicine*, *13*, 69-76.
3. Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial intelligence and machine learning. *Electronic Markets*, *32*(4), 2235-2244.
4. Hunt, E. B. (2014). *Artificial intelligence*. Academic Press.
5. Rockwell Anyoha (2017, August 28). *The History of Artificial Intelligence - Science in the News*. Available at: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ accessed on 6th May 2024
6. Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (Eds.). (2013). *Machine learning: An artificial intelligence approach*. Springer Science & Business Media.
7. *Resilience - Glossary | CSRC*. (n.d.). NIST Computer Security Resource Center | CSRC. Retrieved March 24, 2024, from https://csrc.nist.gov/glossary/term/resilience
8. *Information system resilience - Glossary | CSRC*. (n.d.). NIST Computer Security Resource Center | CSRC. Retrieved March 24, 2024, from https://csrc.nist.gov/glossary/term/information_system_resilience#:~:text=1%20under%20Information%20System%20Resilience,%2C%20contingency%2C%20and%20continuity%20planning
9. *What is Cyber Security? Definition & Best Practices*. (n.d.). IT Governance - Governance, Risk Management and Compliance for Information Technology. Retrieved March 24, 2024, from https://www.itgovernance.co.uk/what-is-cybersecurity#:~:text=Cyber%20security%20is%20the%20application,systems%2C%20networks%2C%20and%20technologies.
10. Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.
11. Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.
12. van den Adel, M. J., de Vries, T. A., & van Donk, D. P. (2022). Resilience in interorganizational networks: dealing with day-to-day disruptions in critical infrastructures. *Supply Chain Management: An International Journal*, *27*(7), 64-78.

13. Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. Ad Hoc *Networks*, *35*, 65-82.
14. Fiksel, J., & Fiksel, J. R. (2015). *Resilient by design: Creating businesses that adapt and flourish in a changing world*. Island Press.
15. 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.
16. Morabito, V. (2015). Big data and analytics. *Strategic and organisational impacts*.
17. 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.
18. Nyström, M., Jouffray, J. B., Norström, A. V., Crona, B., Søgaard Jørgensen, P., Carpenter, S. R., ... & Folke, C. (2019). Anatomy and resilience of the global production ecosystem. *Nature*, *575*(7781), 98-108.
19. United Nations (2024, March 21). *General Assembly adopts landmark resolution on artificial intelligence* The United Nations; Retrieved March 24, 2024, from https://news.un.org/en/story/2024/03/1147831
20. The White House. (2023, October 30). *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence | The White House*. The White House; https://www.facebook.com/WhiteHouse/. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence
21. Roesener, A. G., Bottolfson, C., & Fernandez, G. (2014). Policy for US cybersecurity. *Air & Space Power Journal*, *28*(6), 38-54.
22. Souza, G. (2015). An Analysis of the United States Cybersecurity Strategy. *Center for Development for Security Excellence, Defense Security Service*, 1-29..
23. Street, P. M. O., 10 Downing. (2023, November 1). *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 - GOV.UK*. GOV.UK; 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
24. *The Bletchley Declaration*. (n.d.). The Bletchley Declaration. Retrieved March 24, 2024, from https://thebletchleydeclaration.com/
25. Ministry of Electronics and Information Technology (2023) Proposed Digital India Act, 2023 Available at: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf accessed on 6th May 2024
26. National Cyber Security Policy -2013 Available at: accessed on 2nd May 2024https://static.investindia.gov.in/National%20Cyber%20Security%20Policy.pdf
27. *China's Data Governance and Cybersecurity Regime - ICAS*. (n.d.). ICAS. Retrieved March 24, 2024, from https://chinaus-icas.org/research/chinas-data-governance-and-cybersecurity-regime/
28. PricewaterhouseCoopers. (n.d.). *A comparison of cybersecurity regulations: China*. PwC. Retrieved March 24, 2024, from https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html
29. Data Security Law of the People's Republic of China (n.d.) Retrieved March 24, 2024 from http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html
30. *Cybersecurity Framework & Policies | Microsoft Cybersecurity*. (n.d.). Microsoft – Cloud, Computers, Apps & Gaming. Retrieved March 24, 2024, from https://www.microsoft.com/en-us/cybersecurity?activetab=cyber%3aprimaryr2
31. Intelligence, M. T. (2024, February 14). *Staying ahead of threat actors in the age of AI | Microsoft Security Blog*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

32. *Blog - Advancing iMessage security: iMessage Contact Key Verification - Apple Security Research*. (n.d.). Blog - Advancing IMessage Security: IMessage Contact Key Verification - Apple Security Research. Retrieved March 24, 2024, from https://security.apple.com/blog/imessage-contact-key-verification
33. *OpenAI Cybersecurity Grant Program*. (n.d.). OpenAI. Retrieved March 24, 2024, from https://openai.com/blog/openai-cybersecurity-grant-program

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.