The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES

- ***Chhavi Priya***

ABSTRACT

The rapid advancement of technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and 5G networks has fundamentally reshaped the digital landscape. This transformation, while offering unprecedented benefits, has simultaneously created a new generation of cyber threats that current legal and policy frameworks are ill-equipped to handle. This study provides a comprehensive, multi-disciplinary analysis of these emerging challenges, arguing that a critical disconnect exists between the speed of technological evolution and the static, human-centric nature of existing governance models. The report synthesizes key findings from academic, governmental, and industry sources, highlighting the paradoxical nature of data breach costs, the dual-use capabilities of AI, the unique vulnerabilities of a fragmented IoT ecosystem, and the profound geopolitical risks inherent in 5G infrastructure. The analysis demonstrates that cybercrime is no longer solely about data theft but has evolved to weaponize operational disruption, posing a direct threat to critical infrastructure and public safety. The paper concludes by proposing a framework for urgent legal and policy reform, advocating for an adaptive, technology-specific, and internationally harmonized approach to digital security and resilience. The central recommendation is a paradigm shift towards a regulatory model that legislates for secure-by-design principles, assigns liability to manufacturers and developers, and recognizes cybersecurity as a core component of national and international security strategy.

INTRODUCTION

The digital transformation has become a defining characteristic of modern society, with technology seamlessly integrated into nearly every facet of human life. From critical

infrastructure and healthcare to personal communication and smart cities, interconnected systems have become the backbone of global operations and daily existence. This hyperconnectivity, while a powerful driver of efficiency and convenience, has concurrently expanded the attack surface for malicious actors, creating unprecedented opportunities for cybercriminals and state-sponsored entities alike.[1] The shift from traditional, self-contained IT systems to a complex, multi-layered ecosystem of autonomous and distributed technologies necessitates a new, nuanced understanding of the cyber security challenges that define this era. This report will provide a comprehensive analysis of this evolving landscape, with a particular focus on the profound impacts of Artificial Intelligence (AI), the Internet of Things (IoT), and Fifth-Generation (5G) networks.

The proliferation of these technologies has led to an exponential increase in vulnerabilities. The number of IoT devices is projected to reach over 75 billion by 2025[2], while 5G networks are expected to connect seven trillion wireless devices over their lifetime.[3] This sheer volume of connected devices represents a qualitative change in the threat landscape. The proliferation of endpoints creates an attack surface that is orders of magnitude larger and more complex than ever before.[4] This complexity is a critical problem for both security professionals and policymakers. A single, insecure device can act as an entry point for a large-scale attack, as evidenced by incidents such as the Mirai botnet in 2016, which leveraged poorly secured IoT devices to cause widespread disruption.[5] The data indicates a direct, causal relationship between the rapid adoption of these new technologies and a corresponding rise in systemic security risks.

REVIEW OF LITERATURE

THEORETICAL FRAMEWORKS: FOUNDATIONAL MODELS FOR CYBERSECURITY GOVERNANCE

[1] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws An_Adaptive_Approach, (accessed Sept.14, 2025)

[2] NST, https://www.nccoe.nist.gov/iot, (accessed Sept. 14, 2025)

[3] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220-239. doi:10.14254/2071-8330.2024/17-2/12

[4]EUROPEANPARLIAMENT,https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)697205Spt., (accessed Sept. 14, 2025)

[5] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach, (accessed Sept.14, 2025)

To effectively evaluate the adequacy of existing cybersecurity frameworks, it is essential to establish a baseline of authoritative models. Two of the most widely recognized frameworks are the NIST Cybersecurity Framework (NIST CSF) and the ISO/IEC 27000 series. The NIST Cybersecurity Framework (NIST CSF) is a comprehensive model that provides a common language for managing cybersecurity risk.[6] The framework is built around five core, outcome-driven functions:

Identify, Protect, Detect, Respond, and Recover. The Identify function focuses on developing a thorough understanding of an organization's assets, systems, people, and data to inform risk management decisions.[7] This includes identifying the business environment, stakeholders, and legal requirements, as well as managing supply chain risks. The Protect function is concerned with implementing safeguards to ensure the delivery of critical services, emphasizing data security, access control, and awareness training.[8] The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event through continuous monitoring of systems and assets. The final two functions, Respond and Recover, focus on the coordinated mitigation and restoration efforts following an incident to ensure timely recovery and minimize impact.[9]

The ISO/IEC 27000 series provide an internationally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).[10]

ISO/IEC 27001 sets out the formal requirements for a certified ISMS, including a structured risk management process.[11]

ISO/IEC 27002, which is read alongside ISO/IEC 27001, provides a detailed "code of practice" or a reference set of best-practice controls to guide implementation.[12] A recent revision to

[6] CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, (accessed Sept. 15, 2025)
[7] Luís Bernardo, Silvestre Malta, & João Magalhães, An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF, MDPI, (accessed Sept. 15, 2025; 6:47 PM), https://www.mdpi.com/2079-9292/14/7/1364#
[8] Luís Bernardo, Silvestre Malta, & João Magalhães, An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF, MDPI, (accessed Sept. 15, 2025; 6:47 PM), https://www.mdpi.com/2079-9292/14/7/1364#
[9] ENZUZO, https://www.enzuzo.com/blog/biggest-data-breach-fines, (accessed Sept. 15, 2025)
[10] NIST, https://www.nist.gov/cyberframework, (accessed Sept. 15, 2025)
[11] NIST, https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions, (accessed Sept. 16, 2025)
[12] NIST, https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions, (accessed Sept. 16, 2025)

ISO/IEC 27002, published in February 2022, consolidated the number of controls from 114 to 93 and organized them into four new themes, reflecting current information security practices.28 While ISO/IEC 27002 is not certifiable on its own, it is widely referenced and can be mapped against other standards like NIST, SOC2, and CIS, making it a highly adaptable guide for organizations.[13]

A comparison of these two frameworks reveals their distinct yet complementary approaches. The NIST CSF offers a flexible, outcome-based framework that is adaptable to different organizational needs, while the ISO series provides a more rigid, certifiable standard for a holistic management system. Both models, however, provide the foundational conceptual pillars for managing cybersecurity risks and will serve as the theoretical lens through which the subsequent chapters on AI, IoT, and 5G will be analysed.

REVIEW OF ACADEMIC AND INDUSTRY LITERATURE

A review of the literature on cybersecurity reveals a consistent pattern of vulnerabilities and emerging threats, particularly at the intersection of new technologies. Research indicates a dual-use nature of AI, highlighting its potential for both enhanced cyber defence and sophisticated offensive operations.[14] Studies on IoT repeatedly highlight vulnerabilities like weak authentication mechanisms and the difficulty of applying updates in resource-constrained devices, underscoring a fundamental lack of secure-by-design principles.[15] The security of 5G is a critical area of study, with literature pointing to the physical layer and signaling protocols as new points of weakness that did not exist in previous generations.[16] The literature consistently points to the need for legal and policy frameworks to adapt to these shifts, moving from human-centric to machine-governed realities.[17] A significant theme in legal scholarship is the difficulty of assigning liability and accountability for AI-driven actions and the need for new frameworks to address the challenges of data privacy in a hyperconnected world.[18]

---

[13]Hamed Taherdoost, *Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview*, SSRN, (accessed Sept. 16, 2025; 8:05 PM) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4178718

[14] SECURE FRAME, https://secureframe.com/blog/data-breach-statistics, (accessed Sept. 16, 2025; 8:10 PM)

[15] Sachin Mishra, *Pragya Rathore, 5G Security Challenges & Solutions: A Comprehensive Survey*, 9, IJRTI, 517, 517-518 (2024)

[16] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220- 239. doi:10.14254/2071-8330.2024/17-2/12

[17] NST, https://www.nccoe.nist.gov/iot, (accessed Sept. 14, 2025)

[18] SECURE FRAME, https://secureframe.com/blog/data-breach-statistics, (accessed Sept. 14, 2025; 8:10 PM)

PRESENT STUDY

A. BACKGROUND OF THE STUDY

The digital transformation has become a defining characteristic of modern society, with technology seamlessly integrated into nearly every facet of human life. From critical infrastructure and healthcare to personal communication and smart cities, interconnected systems have become the backbone of global operations and daily existence. This hyperconnectivity, while a powerful driver of efficiency and convenience, has concurrently expanded the attack surface for malicious actors, creating unprecedented opportunities for cybercriminals and state-sponsored entities alike.[19] The shift from traditional, self-contained IT systems to a complex, multi-layered ecosystem of autonomous and distributed technologies necessitates a new, nuanced understanding of the cyber security challenges that define this era. This report will provide a comprehensive analysis of this evolving landscape, with a particular focus on the profound impacts of Artificial Intelligence (AI), the Internet of Things (IoT), and Fifth-Generation (5G) networks.

The proliferation of these technologies has led to an exponential increase in vulnerabilities. The number of IoT devices is projected to reach over 75 billion by 2025[20], while 5G networks are expected to connect seven trillion wireless devices over their lifetime.[21] This sheer volume of connected devices represents a qualitative change in the threat landscape. The proliferation of endpoints creates an attack surface that is orders of magnitude larger and more complex than ever before.[22] This complexity is a critical problem for both security professionals and policymakers. A single, insecure device can act as an entry point for a large-scale attack, as evidenced by incidents such as the Mirai botnet in 2016, which leveraged poorly secured IoT devices to cause widespread disruption.[23] The data indicates a direct, causal relationship

[19] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCH GATE,https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach (accessed September 15, 2025; 8:20 PM)
[20] NST, https://www.nccoe.nist.gov/iot, (accessed Sept. 15, 2025)
[21] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220- 239. doi:10.14254/2071-8330.2024/17-2/12

[22] European Parliament, https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)697205, (accessed September 15, 2025; 8:26 PM)
[23] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCH GATE,https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach (accessed September 15, 2025; 8:20 PM)

between the rapid adoption of these new technologies and a corresponding rise in systemic security risks.

B. STATEMENT OF FACTS

Cybercrime has reached staggering proportions, with reports from the FBI's Internet Crime Complaint Center indicating losses of $10.3 billion in 2022, a significant increase from the previous year.[24]The financial impact of data breaches is significant and complex. The global average cost of a data breach dropped to $4.44 million in 2025, which represents a 9% decrease from the all-time high of the previous year. However, this global average masks a powerful counter-trend in the United States, where the average cost surged by 9% to an all-time high of $10.22 million. This surge is explicitly attributed to higher regulatory fines and increased detection and escalation costs.[25]This presents a powerful counter-narrative to the common critique that legal frameworks are completely ineffective. The evidence suggests that where stringent legal and regulatory mechanisms are in place, they serve as a powerful financial deterrent and a significant cost driver for victims. This implies that strong, enforceable laws are not merely reactive but can actively shape corporate risk management behaviour and, in the long term, may contribute to overall cost reduction through improved security practices.

Specific attack vectors are also evolving. While the human element remains a persistent weakness, involved in over 60% of all breaches, the methods of attack are becoming more sophisticated. Phishing and credential abuse continue to be primary threats, accounting for a significant portion of all incidents. However, the exploitation of vulnerabilities is a rising vector, increasing by 34% in 2025, partly due to zero-day exploits targeting edge devices. Perhaps most significantly, a new era of automated and sophisticated threats is underway, with one in six breaches in 2025 involving AI-driven attacks.

METHODOLOGY

A. OBJECTIVES OF THE STUDY

[24] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCH GATE,https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach (accessed September 15, 2025; 8:30 PM)

[25] Sachin Mishra, Pragya Rathore, 5G Security Challenges & Solutions: A Comprehensive Survey, 9, IJRTI, 571, 571-572, (2024), https://ijrti.org/papers/2405076.pdf

This study has three primary objectives:

- To provide a comprehensive, multi-disciplinary analysis of the cybersecurity challenges and trends presented by AI, IoT, and 5G networks.
- To evaluate the adequacy of current legal and policy frameworks in addressing these emerging threats.
- To propose a framework of actionable suggestions for policymakers, legal professionals, and technologists to mitigate these challenges and build a more resilient digital society.

B. HYPOTHESIS

The current legal and regulatory cybersecurity frameworks, predominantly based on human-led actions and traditional network architectures, are fundamentally inadequate to address the challenges posed by the next generation of autonomous, interconnected, and highly complex AI, IoT, and 5G technologies. A paradigm shift towards adaptive, technology-specific, and internationally harmonized legal standards is required to ensure digital security and resilience.

C. RESEARCH PROBLEMS

The central research problem is the critical disconnect between rapidly evolving cyber technologies and the static, human-centric legal and policy frameworks designed to govern them. This study seeks to address several key issues arising from this gap:

1. How can accountability be assigned when autonomous AI systems make decisions that lead to a cyber incident, and how can attacks be attributed when AI is used to obscure their origins?
2. How can regulatory frameworks effectively address the unique vulnerabilities of a fragmented IoT ecosystem, particularly the lack of manufacturer incentives for firmware updates and secure-by-design principles?
3. How can nations and international bodies mitigate the security risks associated with dependence on a limited number of high-risk vendors for critical 5G infrastructure?

D. DATA COLLECTION AND ANALYSIS

This paper employs a qualitative, analytical approach based on a systematic review of secondary sources. The research material includes a wide range of authoritative documents and analyses, including academic papers and peer-reviewed journals on cybersecurity, AI, IoT, and 5G. In addition, government and intergovernmental reports from agencies such as the U.S. Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the European Union provide a crucial policy perspective. Finally, industry reports and analyses from organizations like IBM, Verizon, and the Identity Theft Resource Center, alongside legal case studies and data on regulatory fines, offer a factual and financial grounding for the analysis. The methodology involves content analysis to identify key themes, patterns, and causal relationships across these diverse sources. The findings are synthesized into a coherent, evidence-based narrative that supports the study's central hypothesis.

THE EVOLVING LANDSCAPE OF CYBER THREATS: TRENDS AND CASES

GENERAL TRENDS AND KEY ATTACK VECTORS

The contemporary cyber threat landscape is characterized by increasing sophistication and a persistent reliance on the human element. While traditional methods remain highly effective, new attack vectors are emerging. Phishing remains a dominant threat, initiating 80-95% of all human-associated breaches and accounting for nearly 30% of global breaches.[26]Credential abuse also remains a common vector, accounting for 22% of incidents. However, there is a marked rise in more complex methods, such as the exploitation of vulnerabilities, which were involved in 20% of data breaches in 2025—a 34% increase from the previous year.[27]

A significant development is the rise of AI-driven attacks, which were involved in one in six breaches in 2025. These attacks primarily leverage AI for phishing and deepfake impersonation. The global average time to identify and contain a breach has fallen to 241 days, a nine-year low, which suggests that security teams and tools are improving their performance in breach detection.[28] However, this improvement is offset by the increasing complexity of

[26] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCH GATE,https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach (accessed September 15, 2025; 9:25 PM)

[27] Sathish A.P Kumar, Mauro Conti, 5G Security Challenges and Solutions: A Review by OSI Layers, RESEARCH GATE, (accessed Sept. 15, 2025; 9:37 PM), https://www.researchgate.net/publication/353938344_5G_Security_Challenges_and_Solutions_A_Review_by_OSI_Layers

[28] Sathish A.P Kumar, Mauro Conti, 5G Security Challenges and Solutions: A Review by OSI Layers, RESEARCH GATE, (accessed Sept. 15, 2025; 9:37 PM),

attacks and the persistent threat of supply chain compromise, which was the second most prevalent and costliest attack vector in 2025.

CASE STUDIES OF MAJOR CYBER CRIME INCIDENTS IN INDIA AND THEIR IMPACT

Digital payments, online retail, e-governance, and vast amounts of institutional and personal data are all becoming more interconnected, making India a target as well as a major user of digital technologies in recent years. Although this change has many advantages, it also reveals weaknesses. Cyberthreats are exacerbated by legacy systems, poorly secured endpoints, a lack of regulatory oversight, and low user awareness. The case studies that follow show how cybercrime has appeared in India as malware intrusions, data breaches, and the illegal trade in personal information, as well as the resulting security, regulatory, reputational, and financial repercussions.

1. Hitachi Payment Services / Indian Bank Debit-Card Data Breach (2016)

Incident: Hitachi Payment Services, a payment processor that serves banks and automated teller machines, had its systems compromised by sophisticated malware in 2016. About 3.2 million debit card details from several large banks, including SBI, HDFC, ICICI, Yes Bank, and Axis, were made public by this hack.[29]

Impacts:

- According to preliminary reports, 641 customers suffered financial losses of roughly INR 1.3 crore.[30]
- Customers were asked to update their PINs; banks were compelled to block and replace compromised cards, particularly for transactions made abroad; and suspicious transactions were subject to heightened scrutiny.[31]
- A worsening of banks' and payment processors' reputations; increased public anxiety regarding the safety of electronic payments.

https://www.researchgate.net/publication/353938344_5G_Security_Challenges_and_Solutions_A_Review_by_OSI_Layers

[29] THE FINANCIAL EXPRESS, financialexpress.com/india-news/hitachi-payment-services-mid-2016-breach-in-india-due-to-sophisticated-malware/544051/ (accessed Sept.18, 2025; 6:24 PM)

[30] Nupur Anand, *Govt orders probe into debit card data breach*, BUSINESS STANDARD, (accessed Sept. 18, 2025; 6:30 PM) https://www.business-standard.com/article/finance/govt-orders-probe-into-debit-card-data-breach-116102001121_1.html

[31] THE FINANCIAL EXPRESS, https://www.financialexpress.com/india-news/hitachi-payment-services-mid-2016-breach-in-india-due-to-sophisticated-malware/544051 (accessed Sept. 18, 2025; 6:32 PM)

- Regulatory ramifications: it caused third-party banking service providers, particularly payment processors, to be closely examined for their cyber security procedures.[32]

2. JustDial Data Exposure (2019)

Incident: It was found that Justdial, a major local search and vendor listing platform in India, had exposed more than 100 million users' personal information through unprotected API endpoints. The exposed data included names, mobile numbers, addresses, email IDs, gender, date of birth, occupation etc. Their system's older versions, which hadn't been patched since the middle of 2015, were vulnerable.[33]

Impacts:

- Extensive disclosure of personally identifiable information (PII), which may allow for social engineering, phishing, identity theft, and marketing abuse.
- Users are worried about data protection and privacy, and public trust has declined.
- Regulatory burden: examination by cyber security and data protection organisations; After being made public, Justdial allegedly conducted audits and fixed the vulnerabilities.[34]

3. Kudankulam Nuclear Power Plant Malware Incident (2019)

Incident: Malware known as "Dtrack" was discovered in September 2019 on an administrative PC connected to the Internet at the Kudankulam Nuclear Power Project in Tamil Nadu. Instead of the plant's vital control systems, the malware was discovered in what is said to be a separate administrative or internet-facing network.[35]

Impacts:

[32] BUSINESS STANDARD, https://www.business-standard.com/article/finance/debit-card-breach-hitachi-owns-up-to-systems-being-compromised-in-mid-2016-117020900504_1.html (accessed Sept. 18, 2025; 6:40 PM)
[33] Shweta Ganjoo*, JustDial data breach: Personal data of over 100 million users exposed online*, INDIA TODAY, (accessed Sept. 18, 2025; 6:50 PM), https://www.indiatoday.in/technology/news/story/justdial-data-breach-personal-data-of-over-100-million-users-exposed-online-1504929-2019-04-18
[34] BUSINESS TODAY, https://www.businesstoday.in/technology/news/story/justdial-data-breach-100-million-users-denies-report-186501-2019-04-18, (accessed Sept. 19, 2025; 7:12 PM)
[35] THE HINDU, https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article61968950.ece, (accessed Sept. 19, 2025; 7:18 PM)

- The incident highlighted vulnerabilities in auxiliary or administrative networks, even in critical infrastructure, even though the core safety or control systems remained unaffected.[36]
- Organisations believed that sensitive systems were isolated, but ancillary networks can serve as attack vectors, raising concerns about "air-gap" assumptions.
- Sparked national discussions on threat intelligence, network segmentation, monitoring, cyber hygiene, and administrative system audits, particularly for critical industries.

4. Illegal Sale of Personal Data via Justdial (2023 Data Theft Case)

Incident: Seven people were detained by Cyberabad Police in 2023 on suspicion of stealing and selling the personal information of 16.8 crores (168 million) people, including PAN card and bank details, government employees, jobseekers, NEET applicants, and defence personnel. According to reports, unregistered businesses were selling the data.[37]

Impacts:

- Potential risks of financial fraud, espionage, and impersonation were implicated by the scope of personal data exposure, which included extremely sensitive categories (government employees, defence personnel).
- Law enforcement raised concerns about the implications for national security.[38]
- In digital ecosystems, it was shown that there was insufficient oversight of data collection, aggregation, storage, and third-party sharing. This led to calls for stronger data protection regulations, audits, and secure procedures.

IMPACT SYNTHESIS

Some broad conclusions can be drawn from these cases:

1. Financial loss is frequently direct but, in most situations, small in comparison to the number of people impacted; occasionally, the harm is greater in terms of possible abuse (fraud, phishing, identity theft).

[36] THE HINDU, https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article61968950.ece, (accessed Sept. 19, 2025; 7:23 PM)
[37] THE INDIAN EXPRESS, https://indianexpress.com/article/cities/hyderabad/seven-held-over-illegal-sale-of-data-of-16-8-crore-people-through-justdial-cyberabad-police-8514920, (accessed Sept. 19, 2025; 7:36 PM)
[38] THE INDIAN EXPRESS, https://indianexpress.com/article/cities/hyderabad/seven-held-over-illegal-sale-of-data-of-16-8-crore-people-through-justdial-cyberabad-police-8514920/ (accessed Sept. 19, 2025; 7:45 PM)

2. Businesses, banks, and operators of vital infrastructure often suffer reputational damage that outweighs the immediate monetary losses.
3. Following significant incidents, there is an increase in regulatory and policy pressures, including calls for stricter obligations for third-party vendors and processors, improved cyber audit mandates, and stronger laws (such as those pertaining to personal data protection).
4. Legal remedies and awareness are still lacking; many victims might not even be aware that their data has been compromised; filing formal complaints, conducting investigations, and receiving compensation are time-consuming.

CYBERSECURITY CHALLENGES AND TRENDS IN AI AND ML

THE DUAL-USE NATURE OF AI IN CYBERSECURITY

Artificial intelligence has a complex, dual role in the cyber landscape, acting as both a powerful tool for defense and a dangerous weapon for offense. On the defensive side, machine learning algorithms can analyze vast amounts of network traffic and user behaviour to rapidly identify anomalies that might otherwise go unnoticed by human analysts.[39] AI-enhanced systems can detect malware, phishing attempts, and insider threats more efficiently and with greater accuracy than traditional methods, providing a critical advantage against increasingly sophisticated attacks.[40]

On the offensive side, however, AI is being used to develop sophisticated hacking tools. AI-driven systems can launch autonomous attacks, identify vulnerabilities in real-time, and create highly targeted, polymorphic malware that changes its code and behavior to evade traditional signature-based detection systems.[41] This ability to adapt and evolve during an attack makes AI-driven offensive capabilities particularly dangerous, as they can continuously improve their effectiveness based on real-time data.

The proliferation of agentic AI, which empowers systems to make decisions without human oversight, makes these threats even more concerning, as a malicious AI could find a way into

[39] SECUREFRAME, https://secureframe.com/blog/data-breach-statistics, (accessed Sept. 20, 2025; 6:12 PM)
[40] FORTINET, https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics, (accessed Sept. 20, 2025; 6:22 PM)
[41] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCHGATE,https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach (accessed September 20, 2025; 6:30 PM)

a victim's network and communicate with the victim's own AI, working in partnership to wreak havoc.[42]

SPECIFIC AI-DRIVEN ATTACK VECTORS[43]

The rise of AI has enabled a new class of attacks that directly manipulate or leverage AI systems themselves.

- **Poisoning Attacks**: These attacks inject fake or misleading information into an AI model's training data, compromising its accuracy and objectivity.
- **Evasion Attacks**: Subtle changes are made to an AI model's input data, causing it to be misclassified and negatively impacting its predictive capabilities.30
- **Malicious GPTs**: Attackers can create or alter generative AI models to produce harmful outputs, such as generating malware or creating fraudulent content for social engineering campaigns.30
- **Deepfakes**: AI is used to create convincing, doctored audio and video for social engineering and impersonation attacks, making phishing and fraud more effective.10

LEGAL AND ETHICAL IMPLICATIONS

The rise of autonomous, AI-driven cyber threats has outpaced legal frameworks, which primarily address human-led actions, leaving a critical legal vacuum. This has created profound legal and ethical challenges.

A key problem is determining who is legally accountable when an AI system makes an incorrect decision that leads to a cyber incident, especially when there is little to no human oversight. Traditional legal theory is built on the concept of human agency and intent. An AI system that autonomously makes a decision leading to a cyber- incident challenges this foundation. Existing liability frameworks often fail to specify whether the developer, the operator, or the AI system itself is responsible for such a failure.[44]The logical progression of this problem is a discussion of whether AI systems should be granted a form of legal personhood, or if a new doctrine of "supervised autonomy" is required, where the human operator or developer is always held responsible.

[42]IT GOVERNANCE USA, https://www.itgovernanceusa.com/iso27002, (accessed Sept. 20, 2025; 6:39 PM)
[43] ISO, https://www.isms.online/iso-27002/, (accessed Sept. 20, 2025; 6:47 PM)
[44] SECUREFRAME, https://secureframe.com/blog/data-breach-statistics, (accessed Sept. 20, 2025; 6:58 PM)

Furthermore, AI can be used to obscure the origin of an attack, making it "significantly more difficult" to attribute responsibility to state or non-state actors. This challenges traditional attribution processes and undermines international law, complicating geopolitical responses. The potential for AI to operate at a scale and speed beyond human control raises concerns about unintended consequences, such as collateral damage from AI-driven cyberattacks or vulnerabilities in AI defense systems being exploited by adversaries.[45] These legal and ethical gaps create a pressing need for updated legal frameworks that can effectively govern AI's use in cybersecurity, balancing innovation with accountability and ethical standards.[46]

CYBERSECURITY CHALLENGES AND TRENDS IN THE INTERNET OF THINGS (IoT)

The rapid growth of IoT devices has created a complex cybersecurity ecosystem with unique risks, threats, and remediation difficulties. IoT differs from traditional IT due to its size, diversity, and long device lifecycles. Vulnerabilities arise from design trade-offs, supply-chain reuse of vulnerable software components, and inadequate mechanisms for secure updates and device management. Systemic features like botnets, supply-chain exploits, and safety-critical infrastructure attacks increase the risk of compromise.

THE EXPANDED ATTACK SURFACE AND UNIQUE VULNERABILITIES

1. **Sheer scale and heterogeneity broaden the attack surface:** IoT systems create numerous interdependent attack vectors by combining various endpoint classes from various vendors. Flaws in firmware stacks or widely used libraries can affect many manufacturers and industries, increasing the chances of compromise and lateral movement, according to incident and ENISA studies.
2. **Frequent and recurring device-level vulnerability patterns**: Common device-level vulnerabilities in IoT include weak credentials, insecure network services, outdated components, inadequate data protection, and lack of device/identity management. Manufacturers' financial and operational limitations contribute to the occurrence of IoT incidents, making them avoidable.
3. **Supply-chain and third-party software risks**: Third-party stacks, such as network stacks, real-time operating system components, and middleware, are frequently

[45] SECUREFRAME, https://secureframe.com/blog/data-breach-statistics, (accessed Sept. 20, 7:10 PM)
[46] FORTINET, https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics, (accessed Sept. 20, 2025; 7:21 PM)

embedded in IoT devices. Hundreds of millions of devices across sectors have been impacted by vulnerabilities in these shared components (such as "Ripple20"), demonstrating how a single compromised library can generate systemic risk that is challenging to address in the field.[47]

4. **Limited update mechanisms and long lifecycles**: Due to either a lack of authenticated update channels or vendor support ending while devices are still in use for years, many IoT devices were not built for frequent secure patching. Therefore, as fundamental mitigations, NIST and ETSI guidance emphasise the creation of strong update/maintenance policies and lifecycle planning.[48]
5. **Operational constraints and physical risks**: Patching may necessitate downtime that operators cannot afford in industrial and medical settings. Further risks are created by physical tampering and a lack of hardware hardening, since attackers with local access can frequently get past lax defences. When comparing IoT security to traditional IT incidents, these domain-specific limitations raise the stakes for safety.[49]

LEGAL AND POLICY GAPS: THE NEED FOR AN ADAPTIVE APPROACH

The creation of a thorough legal and policy framework to regulate the security of the Internet of Things has lagged behind the quick speed of its innovation. Significant gaps have been created as a result, leaving businesses and consumers vulnerable. The difficulties lie not only in draughting new legislation but also in modifying current ones to reflect the particulars of the Internet of Things.

Among the main legal and policy issues are:

1. **Unclear Liability**: It can be very challenging to ascertain who is legally liable for a security breach in an IoT ecosystem that is multi-layered and includes hardware manufacturers, software developers, service providers, and end users. This problem is made more difficult by the supply chain's intricacy.
2. **Inconsistent International Standards**: Although the Internet of Things is a worldwide phenomenon, there aren't any standardised international security standards or laws. Cross-

[47] WIRED, https://www.wired.com/story/ripple20-iot-vulnerabilities/ (accessed Sept. 21, 2025; 6:16 PM)
[48] Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NATIONAL INSTITITE OF STANDARD AND TECHNOLOGY, (Sept. 21, 2025; 6:20 PM), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
[49] Michael Fagan, Katerina N. Megas, Karen Scarfone, Matthew Smith, Foundational Cybersecurity Activities for IoT Device Manufacturers, NATIONAL INSTITITE OF STANDARD AND TECHNOLOGY, (Sept. 21, 2025; 6:20 PM), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

border data flows are made more difficult by this fragmented legal environment, where data gathered in one nation may be subject to different regulations than where it is processed.[50]

3. **Absence of Mandatory Security Requirements**: IoT devices frequently do not have any mandatory security standards, in contrast to some other product categories. Because they are not required by law to incorporate stronger security measures, manufacturers are able to release products with fewer security features.
4. **Privacy Issues and Data Ownership**: There are serious privacy issues with the enormous volume of data that IoT devices gather. The law isn't always clear on issues like data ownership, usage, and obtaining appropriate user consent.

An adaptable legal strategy is required for addressing these gaps. To do this, governments, tech firms, legal professionals, and civil society organisations must work together to develop a framework that can change as technology advances. Aiming to outlaw default passwords and impose more transparency in data handling, initiatives such as the UK's Product Security and Telecommunications Infrastructure Act 2022 and the National Institute of Standards and Technology's (NIST) guidelines are positive steps. But in order to successfully reduce the escalating cybersecurity threats in the IoT environment, a more proactive and globally coordinated strategy is required.

CYBERSECURITY CHALLENGES AND TRENDS IN 5G NETWORKS

5G offers capacity increases, low latency, and machine-type communications in critical infrastructure, transportation, industry, and healthcare. However, it introduces architectural complexity and security implications, increasing attack surface and stakes for supply-chain integrity. To ensure secure deployments, technical design, supply-chain governance, and international policy harmonisation must be implemented concurrently.

ARCHITECTURAL RISKS AND VULNERABILITIES

5G technology has increased the attack surface by moving network functions from dedicated hardware to virtualized, cloud-native software running on general-purpose servers. This increases the risk to telecom infrastructure, exposing it to threats associated with IT/cloud

[50] Iyanu Samuel Ayebo, The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach, RESEARCH GATE, (Sept. 21, 2025; 6:37 PM), https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach

environments. ENISA and NIST identify virtualization, multi-tenancy, and edge compute as major sources of new risk that require cloud security controls applied within telco environments. Network slicing and isolation challenges introduce complex isolation and assurance requirements, while control-plane and signaling vulnerabilities remain persistent in multi-domain 5G deployments. Edge computing and data-proximity risks increase the risk of tampering and local compromise due to the presence of sensitive workloads at the edge. Software supply-chain and shared component vulnerabilities are also a concern, as cloud-native stacks rely on open-source projects, third-party libraries, and common toolchains. Industry guidance stresses secure software development lifecycle practices, continuous monitoring, and coordinated vulnerability disclosure to cope with this reality. Mitigations are shifting from appliance-centric controls to cross-domain, software supply-chain hygiene, stronger identity and attestation for network functions, runtime workload protection, and continuous assurance mechanisms. NIST and GSMA projects and testbeds now emphasize security-by-design for 5G architectures.[51]

SUPPLY CHAIN AND GEOPOLITICAL CONCERNS[52]

The limited number of vendors in 5G networks poses a significant challenge to security, increasing supply chain disruption and raising geopolitical concerns. The European Union's "toolbox" on 5G cybersecurity identified high-risk vendors and outlined measures to address them. The risk of hostile state actors gaining easy entry points through privileged access or pressure on vendors is a concern. China's national intelligence law has prompted countries like the USA to limit the operations of key Chinese 5G vendors, highlighting the need for strategic, technical, and support measures to protect 5G networks.

The EU's reliance on a single vendor poses a risk to supply chains and potential state-sponsored espionage. The toolbox, a non-binding approach, highlights the tension between national sovereignty and a unified, cross-border approach, particularly concerning 5G networks. The Commission's non-binding nature creates inconsistent application across member states and potential exploitable network gaps. Therefore, a unified, cross-border approach is needed.

POLICY RESPONSES AND THE NEED FOR HARMONIZATION

[51] NIST, https://www.nist.gov/news-events/news/2025/06/new-nist-5g-cybersecurity-white-paper-network-security-design-principles, (accessed Sept. 22, 2025; 7:13 PM)

[52] Joyner, T, Blycha, N, Cook, A, Garside, A, Faithfull, M, Tod, O and Lawrence, R., "The Internet of Things", AUSTRALIAN COUNCIL OF LEARNED ACADEMIES, (accessed Sept. 22, 2025; 7:20 PM), https://acola.org/wp-content/uploads/2021/02/acola-iot-input-paper_privacy-security-and-the-iot_joyner-blycha-cook.pdf

1. **India's regulatory instruments and technical certification**: India is actively implementing regulatory instruments and technical certification for telecom equipment, including the Telecom Engineering Centre (TEC) and MTCTE certification regimes, and is also working towards mandatory security certification for 5G network functions.[53]
2. **TRAI, MeitY and sector consultations**: TRAI, MeitY, and sector consultations highlight policy gaps and coordination needs for 5G adoption and digital transformation, highlighting the need for harmonized technical and legal controls.[54]
3. **CERT-In, incident reporting and national cyber posture**: CERT-In's guidance on incident reporting and critical infrastructure security aligns with India's national cybersecurity planning, enhancing operational 5G risk management and promoting collaboration.
4. **Need for harmonization: technical, legal and international**:

India's large and heterogeneous operator market, indigenous vendor initiatives (e.g., Tejas, C-DOT efforts), and participation in global standards make harmonization essential across four dimensions:

- Technical standards and certification: Common testbeds, accepted lab accreditation, and mutual recognition of test reports to avoid duplication and speed secure deployment. (DoT/TEC's MTCTE moves are a partial answer but need international alignment.)
- Department of Telecom: Procurement and supply-chain risk management: Risk-based supplier assessment frameworks and transparent criteria for trusted sourcing to reconcile security and market competitiveness.
- Operational coordination: Cross-agency incident reporting, shared sectoral playbooks, and coordinated vulnerability disclosure processes (CERT-In + operators + vendors).

[53] DEPARTMENT OF TELECOMMUNICATION, https://eservices.dot.gov.in/sites/default/files/2024-11/downloadDocument_20240701164932.pdf, (accessed Sept. 23, 2025; 7:23 PM)
[54] TELECOM REGULATORY AUTHORITY OF INDIA, https://www.trai.gov.in/sites/default/files/2024-11/DIPAAA_23012024.pdf, (accessed Sept. 23, 2025; 7:30 PM)

- International cooperation: Aligning with 3GPP/GSMA best practices and participating in bilateral/multilateral technical forums to share threat intelligence and harmonize mitigation strategies.

CONCLUSION AND SUGGESTIONS

The research establishes that emerging technologies such as Artificial Intelligence, Internet of Things, and 5G networks have significantly reshaped the cybersecurity landscape, creating new vulnerabilities and sophisticated attack vectors. The rapid evolution of these technologies has outpaced traditional legal, technical, and policy frameworks, leaving critical gaps in governance, accountability, and threat mitigation. While advanced solutions like AI-driven defense systems, zero-trust architecture, and quantum encryption show promise, their adoption remains uneven due to high costs, lack of expertise, and inconsistent international standards. A proactive, adaptive, and collaborative approach—combining technological innovation, legal reform, and global coordination—is essential to safeguard digital ecosystems and ensure long-term resilience.

SUGGESTIONS

1. **Policy and Legal Reform**: Governments should strengthen cybersecurity laws to address AI-driven threats, IoT vulnerabilities, and cross-border data issues while harmonizing with international standards.
2. **Advanced Security Adoption**: Critical sectors must implement zero-trust frameworks, secure-by-design principles, and regular vulnerability assessments to reduce risks.
3. **Capacity Building**: Universities and industries should introduce cybersecurity training to address the shortage of skilled professionals and promote public awareness campaigns on safe digital practices.
4. **Public–Private Collaboration**: Enhanced cooperation between governments, private companies, and international organizations is needed for real-time threat intelligence sharing and coordinated incident responses.
5. **Research and Development**: Investment in emerging areas such as quantum cryptography, blockchain security, and AI-based predictive defences should be prioritized to stay ahead of evolving cyber threats.