Human Factors in Cybersecurity, Vol. 168, 2025, 1–11
https://doi.org/10.54941/ahfe1006136

Human Factors and Strategic Approaches in Cybersecurity: Threats for Critical Infrastructures in NIS2 Domains

Kitty Kioskli[1], Leandros Maglaras[1], Theofanis Fotis[1,2], and Emmanouil Varouchas[3]

[1]trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands
[2]University of Brighton, School of Sport & Health Sciences, Centre for Secure, Intelligent and Usable Systems (CSIUS), Brighton, BN19PH, United Kingdom
[3]Department of Management, The American College of Greece, Athens, Greece

ABSTRACT

In 2024, the frequency and severity of cyberattacks surged globally, with a 28% increase in weekly incidents and projected cybercrime losses of $13.82 trillion by 2028. Critical national infrastructure faced heightened risks due to expanded attack surfaces from Industry 4.0 and accelerated digitalization. This paper provides a comprehensive review of cybersecurity challenges across critical infrastructure, healthcare, and advanced technologies, synthesizing research on vulnerabilities and emphasizing actionable strategies. It highlights regulatory compliance, proactive measures like quantum-safe encryption, and practical insights for implementing resilient systems, bridging gaps between academic understanding and real-world applications.

Keywords: Human factors, Cybersecurity, NIS2, Critical infrastructures

INTRODUCTION

In 2024, cyberattacks surged globally, with organizations experiencing an average of 1,308 attacks weekly in the first quarter—a 28% increase from late 2023 and 5% higher than the same period in 2023 (Paul et al., 2023). The financial toll of cybercrime continues to rise, with losses projected to grow from $9.22 trillion in 2024 to $13.82 trillion by 2028 (Dal Mas et al., 2023). Notably, high-impact attacks on critical infrastructure have increased by 140% (Security Statistics, 2024). The expansion of Industry 4.0, coupled with the integration of connected devices and traditional computer networks, has significantly widened the attack surface of critical national infrastructure (CNI). Both state-sponsored hackers and criminal groups are exploiting vulnerabilities, gathering intelligence, and launching disruptive attacks, threatening essential societal functions. Disruptions to CNI can lead to catastrophic consequences, including economic instability, public safety risks, and environmental harm.

To safeguard CNI, the European Union adopted the NIS1 Directive in 2016, requiring Member States to transpose it into national law by 2018. However, inconsistencies in implementation, such as variations in the

classification of essential entities like hospitals and railway operators, created disparities in compliance efforts (ENISA, 2024). Addressing these issues, the NIS2 Directive, effective from 2024, introduces stricter measures across four areas: risk management, corporate accountability, reporting obligations, and business continuity. Additionally, it mandates baseline security measures to address specific cyberthreats. While NIS1 focused on the security of network and information systems, NIS2 adopts a broader cybersecurity framework, encompassing the protection of users and individuals affected by cyberthreats, as defined in the Cybersecurity Act. Key updates include an expansion of regulated sectors for key entities from seven to ten—now including energy, health, public administration, and space—and new sectors for important entities, such as postal services and digital providers (Checkpoint, 2024). These directives aim to enhance cybersecurity across the EU, ensuring the resilience of critical systems while fostering a more cohesive approach to combating escalating cyber risks.

In light of these developments, this paper aims to provide a comprehensive review of cybersecurity challenges and mitigation strategies, focusing on critical infrastructure, healthcare systems, and emerging digital technologies. By analyzing the evolving threat landscape and regulatory frameworks such as NIS1 and NIS2, the paper seeks to bridge gaps in the literature, offering actionable insights for stakeholders. It contributes to the ongoing dialogue on enhancing resilience by highlighting the interplay between technological advancements, policy measures, and operational practices, ultimately equipping organizations with strategies to navigate an increasingly complex cybersecurity environment.

EVOLVING RISKS IN HEALTHCARE: PROTECTING PATIENT DATA AND PRESERVING TRUST IN THE DIGITAL AGE

The integration of digital technology has revolutionized healthcare, offering advancements like electronic health records (EHRs), telemedicine, remote patient monitoring (RPM), and artificial intelligence (AI). These tools enhance patient care, streamline operations, and improve outcomes. However, the shift to digitalization has introduced significant cybersecurity challenges. Sensitive patient data, stored and shared across interconnected systems, is a prime target for cyberattacks. Common vulnerabilities include weak user authentication, endpoint data leaks, and excessive user permissions. Additionally, the rise of the Internet of Medical Things (IoMT) has exposed healthcare systems to heightened security risks, with connected devices like pacemakers and insulin pumps often lacking robust protections.

Ransomware attacks, phishing, social engineering, and insider threats are among the most pressing cybersecurity concerns in healthcare. Ransomware, in particular, has become increasingly sophisticated, combining data encryption with threats to leak sensitive information. Phishing and social engineering exploit human error, tricking employees into granting unauthorized access to systems. Supply chain vulnerabilities, misconfigured cloud environments, and denial of service (DoS) attacks further compound these risks, disrupting critical operations and potentially compromising

patient safety. The rapid expansion of telehealth and AI-driven tools has also introduced new threats, such as eavesdropping on virtual consultations, adversarial attacks on algorithms, and data manipulation.

To address these challenges, healthcare organizations must prioritize robust cybersecurity measures, including stronger data protection frameworks, secure configurations for cloud and IoMT systems, and proactive monitoring for insider threats. Safeguarding patient data and system integrity is essential not only for compliance with regulations like HIPAA but also for maintaining public trust. As the healthcare sector continues its digital transformation, a focus on cybersecurity will be critical to ensuring the benefits of technological innovation are not undermined by the growing complexity and frequency of cyber threats.

GENERATIVE AI AS A TOOL FOR CYBER OFFENSE

Generative AI has advanced significantly with the development of tools such as ChatGPT and Google's Gemini. Despite these achievements, these systems are not immune to vulnerabilities. Although ethical safeguards are integrated into these models, there are multiple techniques that can be utilized to manipulate and exploit their functionalities (Yigit et al., 2022).

Research within the academic literature investigates the vulnerabilities and sophisticated manipulation strategies associated with generative AI. Analyzing these risks reveals critical security challenges linked to the deployment of advanced AI technologies. These challenges include the circumvention of security mechanisms using techniques such as the RabbitHole attack and the compromise of data privacy through rapid injection methods (Adversa AI, 2024). The findings demonstrate that while GPT-4 has made notable progress in natural language processing, it remains susceptible to rapid injection attacks. These vulnerabilities enable attackers to bypass safety protocols, exploiting the model for malicious activities or the dissemination of misinformation.

Gupta et al. (2023) conducted an in-depth exploration of the intricate vulnerabilities in generative AI, focusing particularly on ChatGPT. Their study emphasized that addressing these threats requires a proactive and adaptive approach due to the dynamic and evolving nature of the risks. This underscores the importance of ongoing vigilance and the development of robust mitigation strategies to safeguard against potential exploitation of these technologies. The following section examines how attackers exploit social engineering techniques to compromise generative AI systems by manipulating their response generation processes. These methods aim to bypass ethical safeguards and elicit responses that would typically be prohibited.

SOCIAL ENGINEERING TECHNIQUES TO COMPROMISE GENERATIVE AI SYSTEMS

- **Jailbreaks:** A key concept in this context is "jailbreaking," which involves circumventing the limitations imposed by AI programming to achieve

specific, often unethical, outcomes. The urgency of implementing robust defenses is underscored by findings that demonstrate how adversaries can undermine the intended ethical use of generative AI technologies. Li et al. (2023) showcased how ChatGPT could be manipulated to bypass ethical filters and disclose personally identifiable information (PII) using a multi-step jailbreaking prompt. Their approach leverages Chain-of-Thought (CoT) prompting, breaking complex tasks into intermediate steps, combined with a "Let's think step by step" methodology to circumvent ethical constraints. This strategy highlights the vulnerabilities in generative AI systems when subjected to methodical manipulation. Xie et al. (2023) identified datasets that could facilitate bypassing ChatGPT's ethical safeguards and proposed a defensive mechanism called System-Mode Self-Reminder, based on the psychological principle of self-reminder. This mechanism encourages ChatGPT to act ethically, significantly reducing successful jailbreak attempts from 67.21% to 19.34%. While the current iteration of GPT-4 demonstrates improved resilience to earlier jailbreak techniques, it remains susceptible to advanced manipulation attempts, underscoring the need for continued advancements in AI security and ethical safeguards.

- **Social Engineering:** Falade (2023) examines how generative AI enhances social engineering tactics, enabling attackers to manipulate individuals into compromising security or revealing sensitive information. Tools like ChatGPT, FraudGPT, and WormGPT improve the realism of phishing, pretexting, and deepfake generation, increasing the effectiveness of these attacks. The study highlights the dual-edged nature of technologies such as Microsoft's VALL-E and DALL-E 2, which, while beneficial, are also exploited to create convincing deepfakes and manipulate human cognitive biases. The research traces the evolving threat landscape shaped by generative AI, emphasizing the growing sophistication of social engineering attacks. These advancements challenge traditional security measures and underscore the need for robust countermeasures to address the increasing risks posed by these technologies.
- **Phising Emails:** Begou et al. (2023) analyze how ChatGPT enhances phishing campaigns by automating key components such as website cloning, credential theft code integration, code obfuscation, and automated deployment. Using a threat model that leverages ChatGPT's Python capabilities and OpenAI Codex, the study demonstrates how generative AI accelerates the development and deployment of phishing infrastructure. A case study involving a LinkedIn impersonation phishing site illustrates the practical risks of these advancements, emphasizing the need for robust defenses against the misuse of AI in cyberattacks.
- **Automated Hacking:** PentestGPT (Deng et al., 2023) and GPTs (OpenAI, 2023) are custom iterations of ChatGPT tailored for specific tasks, such as GPTetser and Pentest Reporter, which assist in penetration testing—authorized simulations of cyberattacks to evaluate system security. While these tools are intended for legitimate purposes, they also present a risk of being repurposed for malicious activities in automated hacking. Emerging tools like WolfGPT, XXXGPT, and WormGPT further highlight

the potential for AI models to be leveraged offensively, although their capabilities remain unassessed in comparative studies. Gupta et al. (2023) noted that AI models could analyze new code for vulnerabilities by referencing datasets of known software weaknesses, potentially identifying attack vectors. This dual-use nature of AI tools underscores the risk that malicious actors could exploit similar models to automate unethical hacking practices.

- **Attack payload generation:** Several studies (Yigit et al., 2024) have highlighted the ability of large language models (LLMs), particularly ChatGPT, to generate payloads. Our evaluation of GPT-4 confirmed its proficiency in creating payloads and embedding them into files, such as PDFs, via reverse proxy mechanisms. Key frameworks leveraged by GPT-4 for successful payload generation include the following: Veil-Framework, which creates payloads capable of evading antivirus detection; TheFatRat, a versatile malware compilation tool producing formats like .exe and .apk; Pupy, a cross-platform post-exploitation and remote administration tool; Shellter, which injects shellcode into native Windows applications; Powersploit, a collection of PowerShell modules for penetration testing; and Metasploit, a widely used framework for exploit development and deployment. These capabilities emphasize the utility of LLMs in advanced payload creation while underscoring the potential security risks associated with their misuse.

THE INFLUENCE OF QUANTUM COMPUTING ON CRYPTOGRAPHIC SECURITY

The potential for quantum computing to undermine widely used encryption methods carries profound implications for sectors such as finance, healthcare, government, and technology. Sensitive data in these areas is at risk if it continues to rely on cryptographic algorithms vulnerable to quantum decryption. This looming threat underscores the urgency of adopting quantum-resistant encryption methods, collectively known as post-quantum cryptography. Organizations and governments must act proactively by investing in research, transitioning to quantum-safe encryption, and developing strategies to secure data in a quantum-powered future. Such efforts are essential to safeguarding privacy and security in the quantum age. Key Threats Posed by Quantum Computing:

Information Lifespan: The lifespan of information refers to the length of time data within an organization must remain secure, whether to protect sensitive personal information or safeguard intellectual property. With the looming advancement of quantum computing, threat actors can store encrypted data today, with the intent of decrypting it in the future once sufficiently powerful quantum computers are developed. This poses a significant risk for data with medium to long-term value—information that will still require protection 10 years or more into the future. Such data could become vulnerable to decryption, exposing it to unauthorized access by malicious actors.

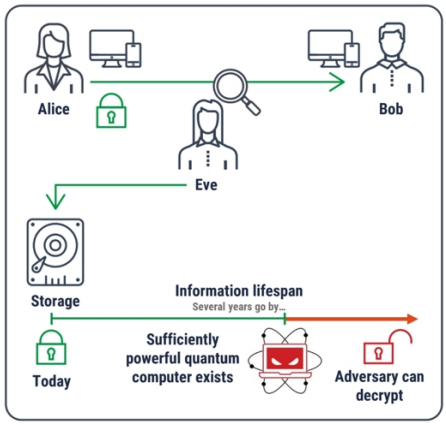

Figure 1: Information lifespan threat (Canadian Center for Cybersecurity, 2023).

Readiness for Quantum-Safe Transition: While the promise of a QS future offers new solutions to counter quantum threats, adapting current cryptographic algorithms and encryption methods within existing infrastructures to quantum-safe alternatives remains a complex challenge. The increasing dependence on secure digital communication and information exchange adds layers of difficulty to this transition. Successfully shifting to quantum-resistant systems requires collaboration across a broad network of stakeholders, including standardization bodies, regulatory agencies, service providers, hardware and software vendors, and end users. These technical interdependencies are critical to ensuring a smooth and effective migration to quantum-safe infrastructures (Lovic, 2020).

Standards & Regulations: The standardization process for QS solution algorithms is still underway and has yet to be finalized. Once these standards are established, the technical components of QS cryptographic algorithms will require thorough validation through extensive testing. Currently, organizations face uncertainty regarding which QS solutions will be officially approved for integration into software and hardware, as well as the timeline for the availability of these new products. This lack of clarity, compounded by numerous technical uncertainties, makes the development of QS technology highly unpredictable. As a result, organizations encounter significant challenges in preparing for the transition to quantum-safe systems (Christiansen at al., 2023). Critical infrastructures are governed by a complex framework of regulations, including international laws, national mandates, technical standards, and operational protocols. The recently introduced NIS 2 Directive builds on the original EU cybersecurity directive (NIS), imposing stricter requirements across the EU to strengthen the security of networks and information systems. Concurrently, discussions around the proposed EU Cyber Solidarity Act aim to further enhance cyber resilience. With non-compliance carrying severe consequences, organizations are legally required to adopt effective measures to address potential security threats and ensure regulatory adherence.

INDUSTRIAL IOT (IIOT): THREATS

The Industrial Internet of Things (IIoT), also known as Industry 4.0, integrates technologies such as smart devices, Cyber-Physical Systems (CPS), and cloud or edge computing platforms to optimize industrial processes by enabling real-time, intelligent, and autonomous data exchange. Industrial Control Systems (ICS), a critical component of IIoT, prioritize availability and integrity to manage processes that directly impact safety, the environment, and financial stability. Unlike traditional IT systems, ICS operations focus on minimizing disruptions in critical infrastructure like power grids and transportation, which can have widespread economic repercussions. IIoT networks are inherently more complex and sensitive than traditional IoT networks due to their larger scale, critical nature, and the integration of diverse industrial components, including SCADA systems, sensors, and Programmable Logic Controllers (PLCs).

Despite its transformative potential, IIoT introduces a wide array of vulnerabilities, particularly in communication protocols, authentication mechanisms, and application security. Common issues include insecure industry protocols (e.g., Modbus, Profibus), poor IT-OT segregation, weak encryption practices, and inadequate security monitoring. Other risks stem from physical security weaknesses, default configurations, and vulnerable PLC operating systems, which can be exploited through weaponized malware. Addressing these challenges requires a comprehensive approach that combines robust security policies, tailored attack detection mechanisms, and close collaboration between IT and OT teams to ensure resilience against evolving threats.

Table 1: Most common cyber threats for each IIoT application domain.

Application Area	Cyberattacks/Threats
IIoT in mining	Cyber espionage; Phishing attack; Third-Party access attacks
IIoT in manufacturing	Ransomware; DDoS/DoS; Spear phishing; Device hacking; Third-Party access; Vulnerabilities in legacy systems; Malware
IIoT in electricity/smart grid	DDoS; Ransomware; Malware injection; MITM; Phishing; Third-Party access; Advanced Persistent Threat (APT)
IIoT in healthcare	Botnets; DoS/DDoS; Ransomware; Third-Party access; APT; Medjacking

Table 2: Actionable insights by sector and emerging technology.

Domain/Technology	Identified Cybersecurity Challenges	Actionable Insights and Mitigation Strategies
Healthcare Systems	- Ransomware, phishing, insider threatsIoMT device vulnerabilities- Weak authentication and cloud misconfigurations	- Implement robust data protection and access controls- Secure IoMT configurations- Proactive monitoring for insider threats- Ensure HIPAA and similar compliance measures are met

Continued

Table 2: Continued

Domain/Technology	Identified Cybersecurity Challenges	Actionable Insights and Mitigation Strategies
Generative AI	- Jailbreaking and ethical bypasses- Phishing automation, deepfakes- Payload generation and social engineering	- Develop adaptive, model-specific defenses (e.g., System-Mode Self-Reminder)Strengthen prompt injection preventionImplement continuous AI ethics audits and filter testing
Social Engineering Attacks	- Enhanced phishing and impersonationCognitive manipulation through deepfakes	- Train employees on recognizing AIenhanced phishing- Implement email filtering with AI detection- Deploy real-time behavioral anomaly monitoring
Quantum Computing	- Future risk of decrypting current encrypted data- Readiness gap for quantum-safe systems	- Adopt post-quantum cryptographic solutions- Begin infrastructure audits and system transitions now- Collaborate with standardization bodies
Industrial IoT (IIoT)	- Insecure protocols (Modbus, Profibus)Weak IT/OT segregation- Vulnerable PLCs and SCADA systems	- Implement security monitoring across OT systems- Enforce strict network segmentation- Regularly patch and test industrial components
Supply Chain Security	- Software injection via open-sourceHardware manipulation (e.g., IEMI)- Thirdparty service abuse	- Conduct third-party vendor audits and code provenance checks- Utilize supply chain risk management frameworks- Shift to secure-by-design manufacturing and sourcing practices

Since the Industrial Internet of Things (IIoT) is integrated into most Critical National Infrastructures (CNIs) covered by the NIS2 Directive, this report highlights several emerging threats associated with its adoption (Tables 1, 2). Many of these threats, such as ransomware, are pervasive across multiple sectors and can impact various application areas. However, certain threats are sector-specific, such as medjacking in healthcare. Additionally, specific vulnerabilities like weaponized Programmable Logic Controllers (PLCs) and web-based malware targeting Remote Terminal Units (RTUs) must be addressed when developing security strategies for digital systems incorporating IIoT devices. Other significant attack types include side-channel attacks, Structured Query Language (SQL) injection, Domain Name Server (DNS) poisoning, IP spoofing, remote code execution, brute force attacks, and reverse engineering.

Supply Chain Attacks: Supply Chain attacks can be split into two big categories: Hardware and software. In Table 3 we briefly present several tactics that can be used to perform a supply chain attack.

Table 3: Tactics to perform a supply chain attack.

Third-Party Software	Exploiting a Vulnerability or Implanting of Malicious Code
Managed Service Providers (MSPs)	Pushing out updates or malware to remotely monitored or managed computers
IT vendors	Installing or injecting malicious code by attacking IT vendors
Partners in a physical supply chain	Implanting a malicious chip/module in a commercial product before it is shipped
Non IT contracting vendor	Using a vendor to gain access to privileged resources of the target organization

A software supply chain (SSC) attack occurs when threat actors embed malicious code into product deliverables by compromising open-source libraries. These attackers insert harmful code into publicly accessible repositories, such as GitHub, which developers commonly rely on to add specific functions to their projects. Although these malicious libraries may appear identical to legitimate ones, they can contain harmful features like enabling boot persistence or opening a reverse shell on remote systems. Since open-source code is often integrated into proprietary software, such attacks can have severe consequences, potentially disrupting the entire software supply chain and affecting government, critical infrastructure, and private sector users.

Hardware supply chain attacks can manifest in various forms, posing significant threats to reliability and security. One such threat is intentional electromagnetic interference (IEMI), where an electromagnetic field is deliberately induced within equipment to disrupt integrated circuits or components. Additionally, non-invasive threats leveraging electromagnetic interference waves of lower amplitude than high-power electromagnetic pulses (HPEM) have been reported, compromising the confidentiality and integrity of devices. Specific risks to IoT systems include command injection attacks on smartphones and smart speakers, signal injection attacks targeting embedded medical devices, vulnerabilities in implantable devices, and threats to autonomous vehicles. Emerging threats also involve manipulating actuator control signals—critical components of IoT devices—to disrupt functionality or gain control.

CONCLUSION

The evolving cybersecurity landscape presents a wide range of challenges that span industries, critical infrastructure, and emerging technologies. This report outlines the scope of threats, from direct attacks on industrial IoT systems to sophisticated software supply chain compromises. Each type of threat underscores the importance of implementing tailored cybersecurity

measures, leveraging proactive threat intelligence, and adhering to sector-specific regulatory frameworks. The rise of generative AI technologies, while offering transformative opportunities, has also introduced new risks. Tools like ChatGPT and WormGPT can be exploited to enhance phishing schemes and automate hacking efforts. Addressing these dual-use concerns requires continuous AI monitoring and the establishment of ethical safeguards to prevent misuse.

In addition to these challenges, the growing potential of quantum computing poses a significant threat to current cryptographic systems. Proactive measures, such as the adoption of quantum-safe encryption and preparation for cryptographic transitions, are essential to protecting sensitive data against future quantum-enabled attacks. This report emphasizes the need for enhanced collaboration among government agencies, private sector entities, and cybersecurity experts to mitigate emerging risks effectively. By fostering cooperation and investing in advanced security measures, organizations can build resilience and safeguard critical systems in the face of evolving cyber threats.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: The 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; the 'A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processes' (CUSTODES) which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; and the 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101158555. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

REFERENCES

Adversa AI. (2024). GPT-4 Jailbreak ve Hacking via Rabbithole Attack, Prompt Injection, Content Moderation Bypass ve Weaponizing AI. Retrieved from https://adversa.ai/, Accessed September 30, 2024.

Begou, N., Vinoy, J., Duda, A., & Korczynski, M. (2023). "Exploring the dark side of AI: Advanced phishing attack design and deployment using ChatGPT." arXiv preprint arXiv:2309.10463.

Canadian Center for Cybersecurity. (2024). Addressing the Quantum Computing Threat to Cryptography. Retrieved from https://www.cyber.gc.ca/en/guidance/addressing-quantum-computing-threat-cryptography-itse00017.

CheckPoint. (2024). Shifting attack landscapes and sectors in Q1 2024 with a 28% increase in cyberattacks globally. Retrieved from https://blog.checkpoint.com/research/shiftingattack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyberattacks-globally/.

Christiansen, L. V., Bharosa, N., & Janssen, M. (2023). "Policy guidelines to facilitate collective action towards quantum-safety." In Proceedings of the 24th Annual International Conference on Digital Government Research (pp. 108–114).

Cobalt.io. (2024). Top Cybersecurity Statistics for 2024. Retrieved from https://www.cobalt.io/blog/cybersecurity-statistics-2024.

Dal Mas, F., et al. (2023). "The challenges of digital transformation in healthcare: An interdisciplinary literature review, framework, and future research agenda." Technovation, 123, 102716.

Deng, G., Liu, Y., Mayoral-Vilches, V., Liu, P., Li, Y., Xu, Y., Zhang, T., Liu, Y., Pinzger, M., & Rass, S. (2023). "PentestGPT: An LLM-empowered automatic penetration testing tool."

ENISA. (2024). Threat Landscape 2024. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

European Parliament and Council of the European Union. (2019). Cybersecurity Act (Regulation (EU) 2019/881). Official Journal of the European Union, L 151, 15–69. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881

Falade, P. V. (2023). "Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks." arXiv preprint arXiv:2310.05595.

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy." IEEE Access.

Li, H., Guo, D., Fan, W., Xu, M., & Song, Y. (2023). "Multi-step jailbreaking privacy attacks on ChatGPT." arXiv preprint arXiv:2304.05197.

Lovic. (2020). Quantum Key Distribution: Advantages, Challenges and Policy.

NIST. (2021). Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, W. Barker, W. Polk, & M. Souppaya (Eds.).

OpenAI. (2023). Introducing GPTs. Retrieved from https://openai.com/blog/introducing-gpts, Accessed September 15, 2024.

Paul, M., et al. (2023). "Digitization of healthcare sector: A study on privacy and security concerns." ICT Express, 9(4), 571–588.

Raheman, F. (2024). "From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security." Journal of Computer and Communications, 12(3), 252–282.

Xie, Y., Yi, J., Shao, J., Curl, J., Lyu, L., Chen, Q., Xie, X., & Wu, F. (2023). "Defending ChatGPT against jailbreak attack via self-reminder." Nature Machine Intelligence, 5, 1486–1496. doi: https://doi.org/10.1038/s42256-023-00765-8.

Yigit, Y., Bal, B., Karameseoglu, A., Duong, T. Q., & Canberk, B. (2022). "Digital twin-enabled intelligent DDoS detection mechanism for autonomous core networks." IEEE Communications Standards Magazine, 6(3), 38–44. doi: 10.1109/MCOMSTD.0001.2100022.

Yigit, Y., et al. (2024). "Review of generative AI methods in cybersecurity." arXiv preprint arXiv:2403.08701.