Journal of Computer Science Review and Engineering | ***ISSN 1694-4488***
Published by AIR JOURNALS | *https://airjournal.org/jcsre*
16/18 Avenue des Longaniers, Quatre Bornes, Mauritius
airjournals@gmail.com; enquiry@airjournal.org

RESEARCH ARTICLE

Emerging Threats and Adaptive Defences: Navigating Cybersecurity's Future in a Hyper-connected World

Kelvin A. Egoh
Computer Science Department, Lynn University, Florida

Citations - APA

Egoh, K. A. (2025). Emerging Threats and Adaptive Defences: Navigating Cybersecurity's Future in a Hyper-connected World. *Journal of Computer Science Review and Engineering, 9(2) 1-11. DOI: https://doi.org/10.5281/zenodo.15599074*

ABSTRACT

In a hyperconnected world, cybersecurity faces a continuous evolution of threats that challenge traditional defence mechanisms. This paper explores emerging cybersecurity threats, including malware, ransomware, phishing, social engineering, and Internet of Things (IoT) vulnerabilities. It delves into the inadequacies of existing cybersecurity defences in addressing these evolving risks and advocates for adaptive defence mechanisms that leverage AI, machine learning, and zero-trust architectures. The paper proposes collaborative approaches, including public-private partnerships and information sharing, as essential to building a robust defence strategy to address future cyber threats. The need for continuous monitoring, real-time incident response, and adaptive resilience strategies is highlighted to fortify digital infrastructures in the face of escalating global cyber risks.

Keywords: *Emerging Threats; Cybersecurity; Hyperconnectivity; Adaptive Defences; Zero-trust Architecture; Internet of Things (IoT) Vulnerabilities*

Copyright: ©2025 The Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

Cybersecurity is influenced by outdated assumptions about computing systems (Thakur & Parameshachari, 2022). New vulnerabilities and attack tactics arise with each technological advancement. The colocation of infrastructure, such as autonomous vehicles at traffic lights, poses challenges (Belaïd, 2024). Small-scale networks mix protocols and systems to protect critical infrastructure in a rapidly evolving framework. These interconnected systems are called hyperconnected. Case studies highlight the need to understand emerging threats, which we refer to as future threats (He et al., 2021). It is crucial to understand the past to navigate the future of cybersecurity. The accelerating evolution of human-computer systems complicates achieving resilient security. Our primary challenge lies in understanding tomorrow's future threats amid today's complexity (Thakur & Parameshachari, 2022). Section 2 will delve deep into the complex interdependencies of topology and interfaces between OT, IT, and governmental agencies. These interdependencies are complex and crucial, as they could amplify disruptions across discrete business and governmental systems if misconfigured. In Section 3, we argue that such escalating threats caught in the keystone of ubiquitous computing also provide an opportunity for ecosystem-inspired adaptive defence mechanisms to evolve. Adaptive defences leverage AI-driven profiling, root-of-trust mechanisms in hardware-supported enclave virtualisation, and cybersecurity operations centre responses to threats (Belaïd, 2024). Architecture, policies, and procedural risk management are all critical considerations. Rather than define an exhaustive program on how such defences are to evolve, we propose proof-of-concept strategies to isolate efforts on the initial dynamics of these escalating threats and proffer guidelines for research (He et al., 2021).

Understanding Emerging Cyber Threats

In recent years, we have witnessed a rapid explosion of novel cyber threats (Shandler & Gomez, 2023). This emerging virus landscape has introduced new risks and demands for digital security infrastructure. As we evolve into a hyperconnected world, the urgency of facing these threats is a growing challenge (Hasan et al., 2021). Identifying emerging cyber factors is essential and urgent in managing risks. This section outlines and categorizes our best cybersecurity threats for better management. Malware and ransomware are the most widespread digital threats. Malware is designed to attack a computer device by replicating itself and infecting other devices. It can infiltrate a network by masquerading as legitimate and safe files and applications, such as spam emails, network links, downloaded apps, and external drive load programs (Ahsan et al., 2022). Most malware is destructive and designed to damage networks, databases, or files. Ransomware is a form of malware that takes data hostage and demands a ransom to enable users to retrieve their data from devices seized by a cybercriminal. Phishing attempts to deceive individuals into providing sensitive information, such as credit card details and personal identifying data. Social engineering is deceptive. In a coordinated attack, social media may be combined with social engineering. Once the scammers gain trust, they launch web-based attacks against normal human behaviour, rather than targeting technologies (Shandler & Gomez, 2023). The rise of the Internet of Things raises significant concerns regarding protection and privacy. Hyperconnection and the potential for communication failures are concerning due to the increased attack surfaces that technology presents. It could involve hijacking a device or a sensor or maliciously causing a network failure (Ahsan et al., 2022). The considerable acceleration of new cyber risks only emphasises the value of the variables related to cyber threats. With the growth of cyber threats, it is essential to recognise and appreciate what constitutes these dangers in general (Hasan et al., 2021). This compares current cyber defence plans that are not exclusively unknown or unseen for the organisations that enact and retain them. This paper aims to delineate the new technological barriers and patterns associated with the rapid emergence of digital technology threats, providing a context for reviewing technological innovations in addressing these new threats.

Malware and Ransomware

Malware emerged with the advent of the World Wide Web and has since evolved into a persistent problem (Baker & Shortland, 2023). There are several types of malwares, but the two prominent use cases — good or bad — are adware, which displays frequent and relentless advertisements, and ransomware, which is capable of encrypting targeted files on a system until the target pays a ransom, typically in cryptocurrency (Lubin, 2022). All malware performs some deleterious function to the standard end user, including data theft, system management, or malware deployment. Backdoors enable secondary malware to infiltrate a host machine and can also facilitate communication with a remote-acting hacker. Droppers are usually fileless and enable another file to download for

a deeper, more comprehensive scan. High-pressure tactics attempt to prompt customers into swift action, whereas scareware employs overt psychological manipulation to achieve the same goal (Force, 2021). A combination of the relative complexity required to create an adequate protection mechanism against modern malware and the income generated through ransom payouts has driven the evolution of ransomware disproportionately more than other types of malwares (Lubin, 2022). In the past, ransomware targeted individuals rather than corporate or government entities (Baker & Shortland, 2023). Preventative measures to ensure the safety of personal data include frequent system backups, installing software only from trustworthy sources, and verifying the legitimacy of downloaded email attachments (Force, 2021). Precautionary action should be taken to prevent the download of malicious software on charity computers. Spreading via email and remote information is typically a malware's first action toward infection (Lubin, 2022).

Phishing and Social Engineering

A well-known, yet remarkably effective, method employed by malicious actors to gain access to systems is phishing (Baig et al., 2021). The attacker uses a spoofed identity to trick someone into providing critical data about a system. Phishers typically pose as trustworthy individuals or entities, requesting sensitive information or encouraging them to download an infected email attachment or click a link that installs the malware (Alkhalil et al., 2021). The attachment may also redirect the targeted individual to a fraudulent site, asking them to provide personal details. There are variants of phishing, such as spear phishing, which targets a specific individual, and whaling, where attackers aim to gain access to the most valuable company assets by targeting top C-suite officers (Jain & Gupta, 2022). Phishing campaigns aim to deceive users into giving access to their digital security by appearing legitimate or exploiting their emotions (Jain & Gupta, 2022). Social engineering fundamentally convinces individuals to divulge confidential or personal information, thereby compromising network security (Alkhalil et al., 2021). Social engineering involves psychological manipulation to help a person commit fraud or manipulate employees into divulging information about a business. Sharing seemingly innocent details, such as a person's workplace, the company's size, or the identity of the IT manager, typically forms part of the research into a company, its working practices, procedures, policies, or staff. The more a person knows about the company and its staff, the greater the chance they have of sounding credible when posing as someone from that company with an urgent need for information (Baig et al., 2021). We should all strive to know precisely what information is being divulged and to whom, and when in doubt, critically assess the legitimacy of the request. There are stories of attackers going as far as printing corporate logos on items and engaging in activities like dumpster diving to gather sensitive information, further demonstrating the lengths social engineers will go to deceive (Jain & Gupta, 2022).

IoT Vulnerabilities

As IoT devices become more ubiquitous in consumers' homes and workplaces, they risk becoming modern-day "Trojan horses," allowing nefarious operators to surreptitiously enter, traverse, and hijack entire networks (Samirah, 2021). User passwords are often hardcoded or reset to default in IoT devices, allowing attackers to quickly crack them with widely available tools (Jurcut et al., 2020). IoT devices may lack standards for encrypting traffic or use out-of-date encryption that can be hacked. A device standard named P2302 lacks basic mechanisms for handling authenticating edge devices (Pal et al., 2020). Incidents have shown how IoT vulnerabilities can reverberate across Internet ecosystems and have tangible "on-people" impacts. In one instance, hackers exploited 100,000 IoT devices to launch waves of distributed denial-of-service attacks against a domain name service provider, temporarily exhausting a critical gateway to the web, rendering dozens of popular websites unreachable, and causing real-world interruptions and slowdowns for numerous users (Jurcut et al., 2020). The Philippines has developed an IoT device cybersecurity labelling program that employs a tiered approach, with more features and restrictions in higher tiers, ensuring that only "secure" devices achieve the higher ratings. It aimed to create standards that vendors must meet, ensuring IoT users had devices including these protections and setting up the pentest lab (Samirah, 2021). Irish and European authorities have established minimum security requirements for IoT devices, including the prohibition of hardcoded default passwords and the requirement for manufacturers to provide a public point of contact for reporting vulnerabilities (Pal et al., 2020). This framework suggests how one might design a coordinated regulatory approach and reflects the need to involve multiple sectors to secure the IoT space and operationalise a systemic way of addressing such a serious risk (Samirah, 2021). Each aspect of the cybersecurity landscape is an arena where adversaries will adapt. Consequently, IoT ecosystems and their IoT devices are among many potential adaptive

chokepoints. In such a rapidly evolving space, new vulnerabilities, attacks, or exploitation methods could emerge swiftly, challenging any guidance or suggestions made here or elsewhere (Jurcut et al., 2020).

The Evolution of Cyber Defence Mechanisms

The first firewalls were conceptually developed in the 1980s because information security threats have always existed to some degree (Thapa & Mailewa, 2020). It was not until the mid-2000s that the concept of network address translation, or stateful packet filtering, was referred to as firewalls. Attackers, however, have been consistently circumventing our Defences. Sometimes, improvements in security measures can minimize the impact of new attacks, but ultimately, the attacker will continue to evade (Chang et al., 2022). What has been surprising is how often cyber Defence has relied on these preventative and reactive mechanisms in the face of new and novel threats over the last 30 years. Systems that define strict security policies are not wrong. However, it has become clear that, in addition to these user-defined policies, there is a need for data-driven behavioural approaches that are adaptive whenever a determination of what is malicious is made (Efe & Abacı, 2022). Figure 1 illustrates the evolution of cyberattacks and Defence mechanisms over the past 10 years (2014-2023). It highlights a steady increase in cyberattacks, alongside the advancement of Defence mechanisms to mitigate these threats. The gap between attacks and Defences indicates the challenges in keeping up with the growing sophistication of cyber threats.

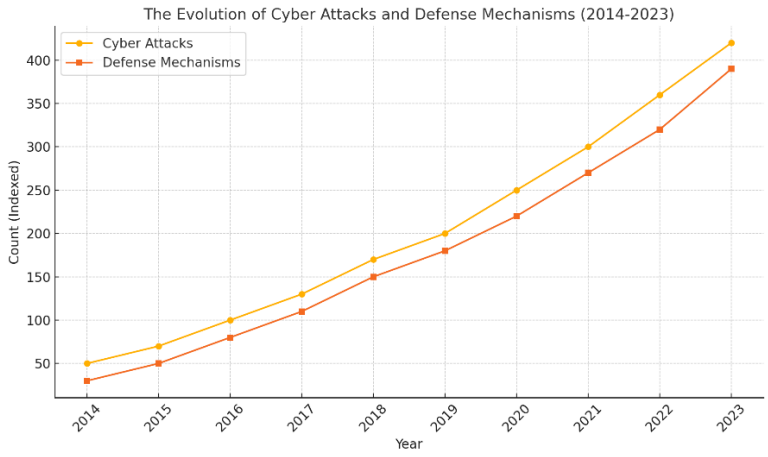

Figure 1: The evolution of cyberattacks and Defence mechanisms from 2014 to 2023.

System administrators primarily utilize two types of traditional Defence mechanisms: firewalls in all their incarnations and intrusion detection systems (Thapa & Mailewa, 2020). One function of virtualizing a machine is to boot a copy of an operating system from a disk. There is a risk of a malicious attack during that boot cycle, potentially causing exploitation. Regarding practicality, system administrators can only afford to dedicate a small subset of computer resources to threat detection (Chang et al., 2022). The necessity of having these “fire alarms” and “locks” in place places a high demand on human analysts, which is why it is risky to take an utterly unsupervised approach to monitoring user activity (Efe & Abacı, 2022). We need to use the behaviour of our users over time to train models to detect and react to unknown attacker activity. Research innovation shows that technological advancements can be made in machine learning, artificial intelligence, visual analytics, resiliency, dependability, and security. These enhancements include predicting human behaviour, identifying deceivers and traitorous individuals, modelling behaviour in standardised systems, and protecting users from cyberattacks (Thapa & Mailewa, 2020).

Firewalls and Intrusion Detection Systems

As science and technology advance, we observe a corresponding growth in our malicious adversaries (Wanda & Jie, 2020). A firewall is "a network security mechanism that can monitor and control incoming and outgoing network traffic based on predetermined security rules" (Sworna et al., 2023). These mechanisms can be anything from a packet filter to an entire proxy server. At its core, the purpose of a firewall is to serve as a barrier between secure and non-secure network operations. Firewalls have traditionally had a quasi-all-or-nothing mentality, where the

traffic is perfectly known and safe or non-compliant with company policies. Any traffic can fit into this simple mould, but no modern organisation operates like that (Bertoli et al., 2021). For some, next-generation firewalls have begun to replace the rigidity of unchangeable firewall rules, but they may still have limitations for more extensive enterprise networks (Wanda & Jie, 2020). Some organisations are using new policies to allow the use of specific software to access their network, assuming all else is a threat. To bridge the knowledge gap between secure environments, intrusion detection systems (IDS) were created to identify potential security breaches (Sworna et al., 2023). These systems have the crucial purpose of monitoring and identifying potential security breaches. Initially, these systems monitored the network for potential attacks, but they have since evolved to protect against host-based threats. Modern methods combine various forms of these two threat identification methods and serve as a response agent when abnormalities are observed in an organisation (Bertoli et al., 2021). In summary, firewalls have remained a foundational network security strategy that ranges from simple to complex, working to prevent threats from entering an organisation's network. IDSS have continued to grow as a correlation and alerting service to the firewall, and often more, with its ability to monitor and respond to changing threats on a large scale (Sworna et al., 2023). We are unconvinced that firewalls are the silver bullet to these issues; they attempt to solve a need to prevent compromise based on hidden knowledge, a trivial approach that is overrun by today's security landscape (Wanda & Jie, 2020). We propose that organisations fortify their castle walls with multiple layers to combat attacks effectively, each working in conjunction with other subsystems to collectively respond to a threat (Bertoli et al., 2021).

Machine Learning and AI in Cybersecurity

In recent years, machine learning algorithms and artificial intelligence (AI) have transformed different sectors, demonstrating substantial improvements in the automation and optimisation of processes (Sarker et al., 2020). Machine learning and AI are closely linked and are often used interchangeably in the tech industry. However, AI is an all-encompassing concept that includes subfields such as cognitive computing, machine learning, computer vision, natural language processing, and robotics (Bagaa et al., 2020). Machine learning, on the other hand, is a subset of artificial intelligence (AI). Machine learning trains a computer system to analyse vast datasets, learn patterns from the data inputs, and leverage the identified data patterns to produce suitable outputs. While not exclusively limited to this principle, AI enables computer systems to learn from experience rather than being programmed to perform explicit tasks (Dushyant et al., 2022). While we dedicate a subsequent section to AI in the cybersecurity context, machine learning generally enables systems to process far more data than could be analysed with more traditional, manual security analytics approaches (Sarker et al., 2020).

Benefits: One of the fundamental benefits of using machine learning in cybersecurity is its ability to help organisations detect and respond to threats more quickly and accurately (Bagaa et al., 2020). Many tools use machine learning to advance cybersecurity in various domains. For example, a global financial services organisation decreased the average time between breach and discovery from four months to 30 days after implementing machine learning and AI cyber technologies (Dushyant et al., 2022).

Challenges: One challenge organisations must consider is the propensity of machine-learning models to develop false positives. Simply relying on automated algorithms can cause systems to flag trivial, everyday actions as suspicious or dangerous, leading to alert fatigue and overwhelming human analysts (Sarker et al., 2020). Furthermore, machine learning algorithms must be continuously updated and require human oversight, as they are ineffective if left to operate passively (Bagaa et al., 2020). Another critical issue to highlight involves the ethical considerations of deploying machine learning algorithms for cybersecurity. There has been a flurry of debate regarding the flawed and unjust algorithms used in predictive policing that disproportionately arrest minorities and perpetuate racism (Dushyant et al., 2022). It is crucial to pose several questions when automated solutions have substantial errors.

Adaptive Defence Strategies

While no bulletproof defence method can secure systems and data in every scenario, researchers and practitioners update organisational considerations to adapt to the changing threat landscape (Sarkar et al., 2022). This challenge is to avoid economic collapse in the event of espionage in a global digital environment where commercial and government systems are all interconnected (Stafford, 2020). An adaptive defence combines an organisation's security metrics, risk strategy, and security investments at any given moment, considering the current threat

environment (Muhammad et al., 2022). Additionally, the following observations apply to the principles of an adaptive defence in the controlled counterintelligence model. First, a defender should not rely upon the agility of an external actor to underpin their defences, as elite adversaries can easily update operational tactics and infrastructure to circumnavigate defensive controls (Sarkar et al., 2022). Second, organisations should adopt a zero-trust model to secure their network, assuming threat actors may reside against their network or within internal systems for an extended period (Muhammad et al., 2022). Third, continuous technical monitoring and human oversight at key points are necessary to ensure that if an attacker breaches network boundaries, they are detected at the earliest possible opportunity, allowing an adaptive response strategy to be developed and executed in near real-time (Stafford, 2020).

In practice, five stakeholder-relevant goals for implementing adaptive defences must allow for the fulfilment of these objectives and contribute to building an adaptive defence strategy to lay the technical groundwork to advance their respective corollary goals. By tightly controlling aspects of operations beyond the perimeter defences of an information environment, entities can limit the damage in all operations after actors engage in counter space, information, or cyber threats (Sarkar et al., 2022). These best practices propose mechanisms to govern and control mitigations that may be deployed under various operational conditions (Muhammad et al., 2022). By shifting to decisive, proactive defensive measures that can be altered quickly and at a lower cost, implementing adaptive defence strategies increases the likelihood of success across the spectrum of conflict for an entity (Stafford, 2020).

Zero Trust Architecture

Zero Trust is an innovative approach to cybersecurity in the modern, fast-paced, and hyper-connected world (Stafford, 2020). Zero Trust is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, even after someone has gained access. The premise behind Zero Trust is that security breaches are not caused by just a few bad actors but by assumed trust built into network architecture (Chen et al., 2020). In response to high-profile breaches over the last several years, many IT organisations are adopting Zero Trust as a policy. As shown in Figure 1, the Zero Trust model operates under the assumption that a threat actor has already compromised any user's systems that have access to the public network (Dhar & Bose, 2021). The most famous and persistent case is the "principle of least privilege," which means that every user and system must carry out its role and responsibility and may access only the data and systems it needs to perform that task (Chen et al., 2020). Another key concept of Zero Trust is micro-segmentation, which separates security perimeters inside an organisation into isolated areas to minimise the impact of any potential disaster (Stafford, 2020).

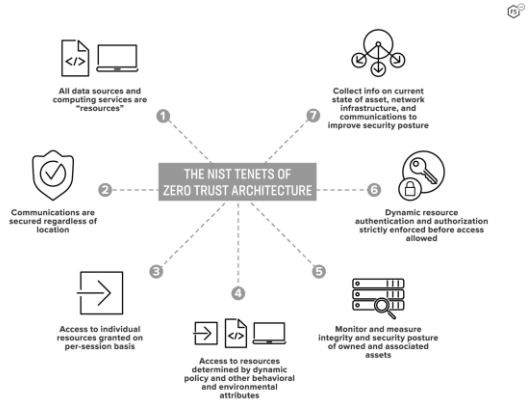

Figure 1: NIST tenets of zero trust architecture (Vinberg, 2022)

Additionally, Zero Trust represents a valuable tool for navigating the rapidly evolving digital landscape. It can help flexible organisations reduce the risk of extortion and significantly limit the impact of any breach with future ramifications (Dhar & Bose, 2021). Technology giants are responding to a significant global event that turns workers everywhere into telecommuters daily (Chen et al., 2020). The Zero Trust system can minimise the error risk by limiting access to only those resources and systems necessary for operations. One of the primary benefits of

implementing Zero Trust use cases is the reduction of network vulnerabilities. Efforts to implement Zero Trust are a perfect example of modernising security frameworks (Stafford, 2020). However, there are boundaries to the zero-trust approach; the availability of resources and the lack of knowledge needed to develop and retain an instinctive zero-trust model are two significant obstacles (Dhar & Bose, 2021). Overall, these statistics reflect the progress that should be made to modernise security frameworks. However, in models and years, cybersecurity represents both an opportunity and an inherent obstacle (Chen et al., 2020).

Continuous Monitoring and Incident Response

Continuous monitoring strategies enhance proactive security defence by enabling the early detection and proactive mitigation of anomalies, thus providing advanced notice of potential threats and ensuring the safety of organisational assets (Maddireddy & Maddireddy, 2020). Organisations must actively engage in comprehensive capacity planning, strategic and operational planning, and meticulous configuration management to establish a robust and effective security architecture (Maddireddy & Maddireddy, 2022). The prompt and efficient execution of incident response protocols is critical in minimising potential damages and legal liabilities. Employing specialised testing and training sessions that accurately simulate crisis scenarios allows an organisation to refine its crisis communication systems and strengthen its preparedness against unforeseen cyber threats (Maddireddy & Maddireddy, 2020). Continuous investment in ongoing training programs and exercises is crucial for effectively mitigating the overall damage caused by cyber incidents and fostering a culture of adaptability in the face of ever-evolving threats (Maddireddy & Maddireddy, 2022). By staying updated on the latest security vulnerabilities and actively enhancing network and system awareness, organisations can ensure they have access to current information on potential security risks. This awareness enables the development of dynamic tools and comprehensive procedures for swift and effective incident response, thereby ensuring the continuity of business operations and safeguarding critical assets against potential harm (Maddireddy & Maddireddy, 2020).

Collaborative Approaches to Cybersecurity

Despite broad global interest in fending off modern cyber threats, organisations face real and practical challenges when operationalising activities necessary to enhance their cybersecurity (Bechara & Schuch, 2021). This section examines the scope and impact of the increasing focus on cybersecurity partnerships. A lone institution cannot adequately address all potential threats it faces. No organisation can collect and analyse event information from all the disparate sources required, nor can it respond to cyber threats comprehensively (Collett, 2021). As a consequence, partnering has become the new norm in the world of cybersecurity. In cybersecurity, partnerships have long been critical for collaborative defence. Economic espionage is an increasingly high-profile cybercrime, often highlighted by state-sponsored hacking activities (Atkins & Lawson, 2021). More nations are aggressively investigating and prosecuting cybercrime, and the corresponding supplier base for law enforcement-related technology has dramatically expanded. Consequently, sharing information about cyber events is becoming more common across the traditional public-private sector line (Collett, 2021). Threat intelligence, defined as knowledge about various activities, tools, tactics, and procedures used by threat actors or attackers, plays a key role in protecting networks (Bechara & Schuch, 2021). Best practices for creating trust environments are derived from traditional threat intelligence-sharing settings, where fostering trust across sectors can often be difficult due to business objectives, industry challenges, and differing motivations. Effective communication facilitates clear, unambiguous exchanges of intent and content (Atkins & Lawson, 2021). Hence, a collective approach to cybersecurity is crucial in a rapidly growing, interconnected world. Unlike other elements of cybersecurity that are in flux, the need to share timely, actionable data from trusted partners remains fundamental (Bechara & Schuch, 2021). The discussion advances the notion of collective cybersecurity by examining mechanisms for sharing data and reporting indicators, including best practices and ongoing research (Collett, 2021).

Public-Private Partnerships

A key component of our effort to counter these threats is to facilitate new forms of collaboration between the public and private sectors (Popoola et al., 2020). As the primary targets of attacks, private network operators—telecommunications carriers, power companies, and digital service providers—are often in the best position to

detect the signs of sprawling attacks long before they encroach on American land, infrastructure, or citizens. Indeed, all manner of sensors and network security products deployed by such entities provide reservoirs of insight which have not been available to previous analysts accustomed to the limits of classified signals intelligence (Ullah et al., 2020). Furthermore, private infrastructure providers possess the resources to conduct effective penetration testing and can make software upgrades and security patches to defend against high-end tools deployed by foreign adversaries (Aljabri et al., 2021). Given that federal agencies often lack these resources and access, it is only logical for these two groups of network defenders to collaborate.

Just as we have called for a broader network of analysts to share in the collective analysis of unclassified data, we believe that over time, there should be increased sharing of information and resources among the public and private sectors in cyber defence. Information sharing, though important, only scratches the surface. There are various ways for the federal government and the private sector to collaborate, and collaborative efforts will differ depending on the industry (Popoola et al., 2020). Not surprisingly, we have had the most success with the defence industrial base, as both parties share similar risks. In this sector, we can share top-secret threat information and various technical defences (Aljabri et al., 2021). Some recommendations are already being applied in industries with a lower classification level and fewer political challenges. To establish a public-private partnership, mutual trust must be established, effective processes must be defined, and agreements must be developed to ensure that each party respects and adheres to their commitments (Ullah et al., 2020). Ultimately, how the federal government and critical infrastructure partners collaborate will depend on the specific mechanisms that are found to be most effective. Historical cases of U.S. collaboration internationally on major cybersecurity threats highlight the potential of rare partnerships, which can be game changers in defending against such threats (Popoola et al., 2020).

Information Sharing and Threat Intelligence

Information sharing is often highlighted as a foundational element of effective cybersecurity (Rantos et al., 2020). Although information is available, the challenge lies in leveraging it to inform situational awareness. Threat intelligence has been studied and defined as the collection of evidence and indicators, the identification of patterns, the analysis of known threat actors, and, finally, the dissemination of the insights gained (Syafrizal et al., 2020). Information sharing and threat intelligence can originate from various sources, including technical sources, hackers and threat actors. Trust within an organisation is critical for effective information sharing, and this foundational trust should extend into cooperation across organisations (Yeoh et al., 2022). Both collaboration and dissemination are necessary to enhance an organisation's awareness of known and potentially unknown threats. This information can serve as baseline data to complement situational awareness. The critical point is that information is highly valued when shared, as one cyber incident is often cross-organisational (Rantos et al., 2020). There are several information-sharing frameworks available. From the perspective of a small business, the Automated Indicator Sharing (AIS) and the initial model developed by Carnegie Mellon University's Computer Emergency Response Team (CERT) constitute at least a minimum standard (Syafrizal et al., 2020). Regarding data privacy, the General Data Protection Regulation (GDPR) outlines principles for the collection of data. It mandates that it be retained only as long as necessary and protected reasonably (Yeoh et al., 2022). As more information is exchanged, there is always potential for abuse, so protocols should align with established standards. These can include governance measures, data validation processes, and mechanisms for sharing, publishing, or subscribing to threat intelligence (Rantos et al., 2020). Effective information-sharing programs not only provide secure and controlled methods for sharing cyber threat intelligence, but they also promote greater collaboration. Case studies have demonstrated that over 500 industry collaborations identified potential virus signatures with moderate to significant industry consensus, ultimately preventing many malicious cyber incidents (Syafrizal et al., 2020).

Conclusion

In summary, this paper discussed the current and emerging threats in cyberspace, affecting both operational technology and the human layer. It focused on the imperative to understand and address these threats and barriers to mitigation, as well as the need for an adaptive defence capability and strategy. Furthermore, it examined public-private partnerships and information sharing as a central component of potential solutions to these threats. Ultimately, the essays in this collection suggest that there are many forms of cyber threats that organisations need

to engage with and that such threats are constantly evolving and modifying. Policymakers, security, and intelligence professionals must be prepared for and proactive in understanding and responding to a complex and layered threat landscape. All these essays share a defining ethical premise: that comprehensive research collaboration, information sharing, and organisational preparation are necessary to confront current and emerging cyber and security threats. We urge cybersecurity authorities and organisations to consider ongoing innovation and adaptation in their professional practice, just as cyber attackers continually innovate. These essays also highlight the critical need for a more proactive, collaborative, and multi-sectoral approach to security risks. In a final reflection, an editorial policy recommendation emphasises that adequate security in the information age must be based on a complex web of interconnections and overlapping conversations between sub-disciplines, sectors, public and private entities, on an evolving threat matrix. Such a move can be our best bet in unsettled times.

References

Thakur, N. & Parameshachari, B. D. (2022). Human-Computer Interaction and beyond: Advances towards Smart and Interconnected Environments (Part II). [HTML]

Belaïd, A. (2024). Human-Machine Collaboration for Incident Response in Cybersecurity Operations for Autonomous Vehicles. African Journal of Artificial Intelligence and Sustainable Development, 4(1), 297–321. africansciencegroup.com

He, H., Gray, J., Cangelosi, A., Meng, Q., McGinnity, T. M., & Mehnen, J. (2021). The challenges and opportunities of human-centred AI for trustworthy robots and autonomous systems. IEEE Transactions on Cognitive and Developmental Systems, 14(4), 1398-1412. [PDF]

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cybersecurity readiness of organisations and its influence on performance. Journal of Information Security and Applications, 58, 102726. [HTML]

Shandler, R., & Gomez, M. A. (2023). The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government. Journal of Information Technology & Politics, 20(4), 359-374. tandfonline.com

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527–555. mdpi.com

Baker, T. & Shortland, A. (2023). The government behind insurance governance: Lessons for ransomware. Regulation & Governance. wiley.com

Force, R. T. (2021). Combating ransomware. Intel Security Group. in.gr

Lubin, A. (2022). The law and politics of ransomware. Vand. J. Transnat'l L.. vanderbilt.edu

Jain, A. K. & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems. [HTML]

Vinberg, M. H. (2022). What Is Zero Trust Architecture?

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. frontiersin.org

Baig, M. S., Ahmed, F., & Memon, A. M. (2021, November). Spear-phishing campaigns: Link vulnerability leads to phishing attacks, and Spear-Phishing electronic and UAV communication scams are targeted. In 2021, the 4th International Conference on Computing & Information Sciences (ICCIS) (pp. 1–6). IEEE. [HTML]

Samirah, K. (2021). Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme. ncirl.ie

Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. SN Computer Science. [PDF]

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the Internet of Things: A systematic approach. Sensors. mdpi.com

Thapa, S., & Mailewa, A. (2020, April). The role of intrusion detection/prevention systems in modern computer networks: A review. In Conference: Midwest Instruction and Computing Symposium (MICS) (Vol. 53, pp. 1-14). easychair.org

Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., ... & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. Future Internet, 14(3), 89. mdpi.com

Efe, A. & Abacı, N. (2022). Comparison of the host-based intrusion detection systems and network-based intrusion detection systems. Celal Bayar University Journal of Science. dergipark.org.tr

Sworna, Z. T., Mousavi, Z., & Babar, M. A. (2023). NLP methods in host-based intrusion detection Systems: A systematic review and future directions. Journal of Network and Computer Applications, 103761. [PDF]

Wanda, P., & Jie, H. J. (2020). A survey of intrusion detection systems. International Journal of Informatics and Computation, 1(1), 1-10. respati.ac.id

Bertoli, G. D. C., Júnior, L. A. P., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., ... & De Oliveira, J. M. P. (2021). An end-to-end framework for a machine learning-based network intrusion detection system. IEEE Access, 9, 106790-106805. ieee.org

Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A Machine Learning Security Framework for IoT Systems. IEEE Access. ieee.org

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. Journal of Big Data, 7, 1–29. springer.com

Dushyant, K., Muskan, G., Annu, Gupta, A., & Pramanik, S. (2022). Utilising machine learning and deep learning in cybersecurity: an innovative approach. Cyber security and digital forensics, 271-293. [HTML]

Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), 11213. mdpi.com

Stafford, V. (2020). Zero trust architecture. NIST special publication. nist.gov

Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defence, and global standards for a resilient digital future. International Journal of Computer Science and Technology, 6(4), 99-135. researchgate.net

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M. & Zhai, Y. (2020). A security awareness and protection system for 5G competent healthcare based on zero-trust architecture. IEEE Internet of Things Journal, 8(13), 10248–10263. nih.gov

Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. Journal of Organisational Computing and Electronic Commerce, 31(1), 18–34. academia.edu

Maddireddy, B. R., & Maddireddy, B. R. (2020). Proactive Cyber Defence: Utilizing AI for Early Threat Detection and Risk Assessment. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 64–83. ijaeti.com

Maddireddy, B. R., & Maddireddy, B. R. (2022). Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. Unique Endeavour in Business & Social Sciences, 1(2), 47–62. unbss.com

Bechara, F. R. & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime. [HTML]

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence-building measures. Journal of Cyber Policy. tandfonline.com

Atkins, S. & Lawson, C. (2021). Cooperation Amidst Competition: Cybersecurity Partnerships in the US Financial Services Sector. Journal of Cybersecurity. oup.com

V. O. Popoola, A. V. Adebayo, O. C. Oyedeji, M. A. Moronkunbi Digital Economy and Job Sustainability in Nigeria: Challenges and Solutions International Journal of Innovative Science and Research 9 (5), 3114 - 3122

Ullah, K., Rashid, I., Afzal, H., Iqbal, M. M. W., Bangash, Y. A., & Abbas, H. (2020). SS7 vulnerabilities—a survey and implementation of machine learning vs rule-based filtering to detect SS7 network attacks. IEEE Communications Surveys & Tutorials, 22(2), 1337-1371. researchgate.net

Aljabri, M., Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M. & Altamimi, H. S. (2021). Intelligent Techniques for Detecting Network Attacks: A Review and Research Directions. Sensors, 21(21), 7070. mdpi.com

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Challenges to Interoperability in the Cybersecurity Information Sharing Ecosystem. Computers, 9(1), 18. mdpi.com

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standards and framework components. International Journal of Communication Networks and Information Security, 12(3), 417-432. academia.edu

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. Computers & Security. google.com