CyberSystem Journal *Original Article*

Advancements in Cybersecurity: Novel Approaches to Protecting Against Emerging Threats and Vulnerabilities

Atheer Alaa Hammad[1], Hadeel M Saleh[2,3*], and Mohammed F. Alomari[4,5]

[1] Ministry of Education, Anbar Education Directorate, Anbar, Iraq.
[2] National School of Electronics and Telecommunications, University of Sfax, Tunis
[3] Continuing Learning Center, University of Anbar, Iraq
[4] Department of Computer Techniques Engineering, Mazaya university college, Thi Qar, Iraq
[5] Education Directorate of Thi Qar, ministry of education, Iraq.

***** Corresponding Author: Hadeel M Saleh, Email: haddeel.mohammed@uoanbar.edu.iq

***Abstract*:** Cyber threats have expanded from theft of information to the misuse of turned data for intent to manipulate business exposures or to harm and disrupt healthcare operations. Globally, the medical cybersecurity market is $12.6 billion. It is required that medical device manufacturers integrate cybersecurity during the design phase of the product life cycle. Cybersecurity should not have been an afterthought. It is a continuous process that works best if all involved listen to one another. Solutions, technology, and methodologies exist but are not utilized across the healthcare industry to build Cybersecurity by Design medical devices. A risked-based approach is proposed where medical devices are designed, tested, manufactured, and operated with strong consideration of security. The operators and staff should be instructed about the dangers of not operating the device properly. The network surrounding the device should be safeguarded as one part of a wider cybersecurity chain.

Access this article online

***Keywords*:** Architecture, Cybersecurity, Disrupt Healthcare, Virus

1. Introduction

1.1 Background and Significance

The rapid advancements in both Information Technology (IT) and Industry 4.0 have led to a remarkable increase in the inter-connectedness of physical devices; however, this has also prompted a steadily growing number of security threats. Unlike the traditionally ubiquitous IT systems that were under the exclusive control of highly skilled personnel, the new Industrial Internet of Things (IIoT) paradigm proposes the incorporation of a massive number of Industrial Control Systems (ICS) that will function independently, communicate with one another, and therefore potentially operate outside the scope of direct supervision [1]. Although such an environment would be highly beneficial with respect to increased economic profitability, it comes at a high cost in terms of security vulnerability. ICS have mainly been designed with safety as the first, and often sole, priority. On the other hand, the protection of data integrity, authenticity, or confidentiality was usually ignored, as it was assumed that the system was too specialized and closed for unauthorized access. Unfortunately, either naive or negligent assumptions cannot stop cyber terrorists who would easily be able to exploit existing vulnerabilities [2].

Effective countermeasures are necessary at two separate levels. On the one hand, in order to mitigate the risk of exposure to the existing vulnerabilities, the wide variety of devices that are used in such environments should be classified with respect to their security characteristics. Data gained from a thorough investigation of each class would enable the proposal of hardware/software countermeasures

Received February 16, 2024; Revised March19, 2024; Accepted April 24, 2024; Published June 30, 2024
https://doi.org/10.57238/r15e5074

that would increase the resilience of such devices within their targeted environments. On the other hand, the paradigm of IT-driven design and manufacturing is itself responsible for the majority of the risk [3]. Therefore, the fundamental IT-driven design philosophy should be questioned, and novel designs should be proposed for safety-critical devices that would essentially differ from contemporary implementations. Techniques for safe commissioning and validation would also have to be developed [3].

1.2 Research Objectives

The rapid advancement and widespread use of technologies, particularly the internet and web, have considerably affected all aspects of life, changing the way people interact and live. However, while technologies have made a significant contribution to doing tasks faster and better, they can also be dangerous, as people may misuse them for their detriment. The phrase people use to denote accidental or intentional harms arising from emerging technologies is “dangerous”. A broader notion, Pervasive Computing Environment (PCE), is used to denote inherent or impregnable dangers arising from ubiquitous technologies that observes places (“smart” buildings), objects (RFID tags), and even people, tracking them and interfering with their lives [4]. Suggested approaches to protect against two types of PCE dangers, information-related and identity-related, are presented.

The aim of this research is to present novel approaches to controlling two types of the PCE dangers arising from the vanishing of the information others may gather about individuals or groups of people, and to construct such approaches. Additionally, it is addressed the identity-related dangers, including fake-identity problems which were impossible to clear up. Common to the identity-related problems of both types of PCE dangers are PCE roles taken over by devices, namely, observers, assistants, and impersonators. A theoretic framework for studying devices taking over an PCE role is designed, and a complete and coherent treatment of these roles is provided.

2. Foundational Concepts in Cybersecurity

Cybersecurity is critical for the effective functioning of the nation’s infrastructures. Assets such as government and business information networks, transportation systems, electric power grids, medical facilities, and financial institutions are all vulnerable to threats, and the processes employed to manage, control, and protect them are interlinked [5].

Foundational concepts in cybersecurity are introduced to provide a basic knowledge framework upon which the novel topics that follow may be understood and perceived. The fundamental concepts and principles of cybersecurity are discussed with the intention of establishing a common understanding of the essential elements of cybersecurity.

2.1 Basic Principles of Cybersecurity

Cybersecurity refers to a collection of practices, techniques, and concepts that aim to protect systems, networks, devices, programs, and users from unauthorized access, adversities, and many types of cyberattacks [3]. Used in a broader sense, cybersecurity entails the inclusion of layers of protection within the technology and computing systems and is employed to prevent both intentional and unintentional breaches of sensitive information. Cybersecurity has evolved over the decades due to the advent of new technologies and tools, sophistication of cyberattacks, even more stringent guidelines and regulations related to the protection of sensitive data. Basic principles and foundational theories in cybersecurity are discussed in this article.

The basic idea of cybersecurity is analogous to that of a multi-layered protection of a person or a place. Consider a high-profile witness under protection by a team of skilled protection agents. A thorough protection protocol would contain multiple layers in preventing a possible attack on the witness. The first layer might enclose the entire property of the witness with a strongly fortified wall. Guards would stand anywhere on this wall to keep an eye on any suspicious acts outside. In addition, motion and sound sensors would be carefully placed on the wall, ready to send alert signals to choosing response teams when someone crosses the wall. Though this wall looks attractive by itself, attackers are likely to find ways to overcome the wall. One possible way would be to use vehicles with heavy force, such as bulldozers and grenades, to demolish the wall. Therefore, there should be at least another back-up layer for the first wall layer. Inside the wall, there could be a few hidden paths leading away from the property. A covert team of guards would surveil these hidden paths to warn the key persons just in the beginning of attack attempts. In summary, the cybersecurity paradigm considers both the preventative and responsive measures to protect the assets from adversaries.

2.2 Common Types of Cyber Attacks

Those tactics, techniques, and procedures commonly used to exploit considered or discovered vulnerabilities are referred to as security attacks. A cyber-attack is an attack launched from one or more computers against another computer with the intent of harming the targeted computer or network. There are different types of cyber threats and attacks; some of them change coats often but have some similarities with the old ones. Understanding the different types of cyber threats and attacks is vital for the proper constructions of defenses against the common threats [6].

Worm: A worm is a standalone malware computer program that replicates itself in order to spread to other computers. Unlike viruses, it does not need to attach itself to an existing program. Worms exploit vulnerabilities in

operating systems to gain access to computer systems, consuming the target computer's bandwidth slowing it down or even making it unusable [7].

Rootkit: A rootkit is a collection of computer software, typically malicious, that enables continued privileged access to a computer while actively hiding its presence. The term rootkit is a portmanteau of "root," a Unix-like systems administrator account, and "kit," which is a difficult collection of software components. Rootkits can be installed by someone remotely accessing a terminal window on the computer (door), infecting the computer with a virus/ trojan/hacker tool, and gaining "root" access to the system unstructured. Once installed, rootkits allow an administrator to install backdoors (nonsecret access points) to computers making re-entering the broken computer system easier.

Vulnerability scanners: Vulnerability scanning is an automated process to identify a vulnerability in an operating system, application, or network infrastructure. Using this information, the auditors can recognize which prescriptions should be implemented to limit or mitigate potential threats.

Virus: A computer virus is a computer program that can replicate by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then called "infected." The term is widely used to refer to malware that infects other systems or computer applications. Unlike worms, viruses do not copy themselves and spread independently. The virus needs a host computer program to run and executes its code to infect the host. Normally, a virus infects a host file, and when the host file is executed, the virus runs too, and following its instructions, it can replicate, infect other files, or perform other actions on the computer.

3. Traditional Approaches to Cybersecurity

Historically, there has been a visible proliferation of the Internet and timely developments in the Ultra-high-speed Fiber Optic Communication System. Today, not only countries, but also shopping complexes, multi-storied buildings, railway stations, aerodromes, commercial ships, industries, etc., use computer networks for easy and fast flow of data [8]. Unfortunately, this present scenario has vastly enhanced opportunities and scope for criminals to intrude into networks, and thereby cause destruction, loss and exploitation of several assets like hardware, software, data and information, and also human lives. A majority of countries of the world are now a direct or indirect victim of these crimes; and for the past few years, this phenomenon is growing in intensity. Thus, rising incidences of cyber-crime have become a matter of concern for all. Derogation of privacy, unauthorized data alteration or destruction, data theft, stealing of financial information from clients, etc., are some of the vital consequences of cyber-crimes [9]. The present Internet scenario worldwide is reminiscent of the 19th century Gold Rush in the United States. Similar to the Gold Rush, which has led to innumerable roadside robberies due to absence of law and connected deterrent factors, the current exposure of vulnerabilities in computer networks has also created scores of opportunities for computer criminals on an international scale.

In computer networks, intrusion detection is a vital security issue. Conventionally intrusion detection is done (humanly) by network admin or system admin. This kind of intrusion detection has its own drawbacks such as slow response to attacks, lack of consistency and robustness, lack of the ability to analyze on a large scale, etc. To overcome these shortcomings, Automating Computer Network Intrusion Detection Systems (ACNIDS) has been, and still is, one of the foremost concerns of scientists and engineers in information technology. Of late, usage of supervisory control and data acquisition (SCADA) systems in several critical infrastructures have been observed, thus, exposing them to potential cyber threats.

Perimeter protection is the first layer of protection consisting of a firewall enterprise store. This mechanism restricts unauthorized users to connect to the network by defining what users are allowed in and what connections they can make. It defines the policies for which ports to filter and the direction of the filtering, input or output. It also states what services such as ftp, telnet, etc., the predefined user can get access to. A properly configured firewall will prevent 95% of the attacks on a network. Most commonly a firewall is implemented in a screen arrangement of the routers with a proxy service in between. The proxy acts as a gatekeeper, every packet coming in or going out of the network only does so via the proxy. The main focus of any firewall configuration is to deny all and permit few. Such setups will only fail if there is a major error in the configuration. Problems will arise when establishing connections that need to open gates in firewall to access additional machines.

After perimeter protection, an IDS is the second layer designed to identify possible intrusions and network compromise. An IDS passively analyzes network traffic and compares it against a database containing signatures of attack patterns. If a match occurs then the IDS alerts that an attack is suspected. Tuning an IDS device is required to minimize false alerts. Statistics show that a properly tuned IDS will produce only 1% false alert and 15% missed alerts. The IDS will also collect forensic information such as log files which can be useful in the investigation. The latest trend in IDS technology is moving towards an intrusion protection system (IPS). In this kind of system, the IDS not only monitors the traffic but actively blocks packets once an attack is detected. This kind of system cannot currently handle zero-day exploits, but updates can be issued to IPS signatures to defend them. Additionally, in a non-production environment tested signatures can be developed to implement.

3.1 Firewalls and Intrusion Detection Systems

Firewalls and Intrusion Detection Systems (IDS) are widely used as defensive mechanisms to protect networks from intrusions. Firewalls are defined as the edge of a network, which implements rules to decide whether to deny or allow access to information between networks [10]. On the other hand, Intrusion Detection Systems (IDS) are characterized as sensors to detect intrusions or attacks after the firewall and can provide alerts to these attacks. The IDS service can be considered a value-added service since it provides higher visibility into potentially malicious and annoying activity that the firewall would typically allow or ignore. Because most commercial IDS are expensive and require significant resources to monitor a network continuously, they are simply unfeasible to install on most small networks. This is where free and open-source IDS comes into play. There are several free or open-source IDS packages currently available. Some of these have been around for a while, while others are relatively new. This paper seeks to explore how these packages could come together and work as a team to plug a network's vulnerabilities.

The term firewall broadly refers to the edge of a network that implements rules to decide whether to deny or allow access to information between networks. Network behavior or traffic patterns are usually used to develop such rules. A firewall uses this information to analyze each individual packet or stream of packets, including analyzing packet headers for information like the source address, destination address, protocol type, and service type. Based on this analysis, packets are either sent through (allowed) or blocked (denied) access to the network behind the firewall. Given that many attacks exploit open ports and services, firewalls restrict traffic by blocking unauthorized ports or protocols. However, well-configured firewalls cannot fully protect computers under their domain as they primarily use predefined filters and rules for analysis [11]. Thus, if an action does not violate any of these rules, it is allowed, making it almost impossible to stop all unwanted packets from crossing a network boundary.

3.2 Antivirus Software

Antivirus software has become one of the major components of cybersecurity. Antivirus software detects and removes spyware, adware, worms, trojans, keyloggers, and viruses and mitigates several cybersecurity threats. In most cases, modern-day computers have antivirus software which helps stopping attacks before happening. But does it work? How effective are antivirus programs in the modern day? This part attempts to answer these questions [12].

Antivirus is the software that has a database of thousands of known viruses with their signature patterns. The antivirus scans all the data coming in from outside, specifically from the internet. When it finds a match between the incoming data and the virus signature patterns in its database, it flags that data as a virus. According to Mark Meadows, founder of WellinTech, a well-known and reputed company in data acquisition and control, antivirus programs are to be understood as "the shield that protects the computer from attacks" [13]. However, as time is passing by, and viruses are becoming sophisticated with the help of new technologies, the efficiency of the antivirus programs is being compromised. Antivirus programs can block 66% of some identified viruses by several tests. The battle between viruses and antivirus software has been going on for several years. The virus detectors are becoming smarter and the virus creators are finding a way to stay out of the limelight of the antivirus programs. Hence, with the help of the research done here, a digital picture of the effectiveness of the antivirus programs is attempted to be framed.

4. Emerging Threat Landscape

The rapid growth and adoption of the Internet of Things (IoT) have shifted the focus in cybersecurity research to the security of smart devices, with a special emphasis on their privacy, safety, and security. On the one hand, the IoT is an ecosystem of many devices. Most IoT devices are small, smart, and have wireless radio connectivity capabilities with low battery capacity. Most IoT devices are found in everyday objects, with limited computing power, and are often not supported by a proper operating system. Due to these limitations, IoT devices suffer from security issues. The intersectioning nature of IoT systems, including the numerous components required in the deployment of IoT systems, comes with added security challenges. Although significant security measures have been implemented for traditional systems, IoT security is still under research. IoT security is essentially a combination of network security, wireless security, and mobile system security.

Artificial Intelligence (AI) is being harnessed to improve threat detection in existing security settings. AI is used increasingly in the detection of threats on IoT networks and devices due to the rapid growth of the number of connected devices, which creates overhead for system administrators. The current threat landscape is composed of both insecure IoT devices (insecure by design) and malware aware of the unique configurations of networks formed by the cohabitation of IoT devices [14]. As a result, in addition to the generic threats of the Internet worldwide, the new threat provides an attack surface for cybercriminals.

The deep learning techniques introduced by large companies such as Google and Facebook have recently generated significant discussion in the cybersecurity area. These Internet giants have ignited debate about the powerful machine learning techniques they developed, the implications regarding the usability of such tools, and the strategies for countering threats and protecting national protagonists. The machine learning and AI paradigms supporting such systems could enhance their capabilities to adapt.

4.1 IoT Security Risks

Cybersecurity has become a complex and ever-evolving issue in the last decade. Wireless technology has become more pervasive in people's lives, resulting in new vulnerabilities and attack surfaces. Devices such as smartphones and tablets, though originally designed with security in mind, were often thought of as "computers in your pocket" and not directly connected to a global wireless ecosystem. However, with the ubiquity of Wi-Fi and widespread usage of social media, this changed. Almost overnight, a new class of headless devices (IoT devices) exploded onto the scene. IoT devices come in many shapes and sizes, with many different uses, and each one introduces its own risks [15].

As users become reliant on consumer IoT devices (CIDs) in their homes, and as these devices become involved in more critical tasks and sensitive data, such as home security and/or credit card transactions, they also become of more interest to attackers. Key aspects of the risks associated with these devices are the vulnerabilities each device profile introduces to the home network as a whole, and how these concerns are compounded by the unique cyber ecosystem brought on by their introduction. It is not possible to compare the risks of these new devices with older devices, and/or to make assumptions about their risks due to their device profile types [16].

This section aims to open with an in-depth analysis of the risks associated with a few consumer IoT device types. It continues with a broader discussion of the vulnerabilities such devices introduce to home and consumer network security, and aims to close with a contingent amplification of these risks as they are multiplied in IoT ecosystems as a whole.

4.2 AI and Machine Learning Threats

Artificial Intelligence (AI) and Machine Learning (ML) have been increasingly applied in a wide range of industrial and research applicability. On their positive side, AI/ML techniques have been applied to many fields with significant success, but there are sides of this technology that attack unknown aspects. This paper focuses on using AI/ML in Cyberspace technologies and cybersecurity (CY) InfoCon technologies and cybersecurity, presenting Automation Applications in Cybersecurity (AAC) on their disadvantages. There are several threats that AI/ML pose on the basic working principles of the Internet and Information Technology (IT); known as Artificial Intelligence (AI) and Machine Learning (ML) Threats Urbanization, IoT, big data, and AI/ML applications in the industrial field enhance the understanding and knowledge of the city [17]. Here, anything can be connected quickly and flexibly via the internet, opening the opportunity for monitoring, controlling, and optimizing the complex component process at the city level. However, this numerous and complex structure exposes many different and more vulnerabilities and risks as well. Exceptionally, attacks and malware use intelligence and creativity, enhancing the potential of their success [18].

The Cyber Technology (CT) industry has been aware of this kind of programming and has made an enormous effort, but still very cautiously, to prevent and dismiss these potential MAT [19]. This paper presents the rapidly growing immediate threats in Cybersecurity networking, focusing on Ground and Airborne UAV systems. In new Electronics/Wave process applications with internal Internet connections and Cyber Technological Connectivity, Human Connectors are shifted from human dominance in controlling and observing gathering data outputs, protecting from physical devastation, social disruption, and financial loss. If a hacker-supported AI program implements a Critical Infrastructure Transportation defense system or utilizes the CIA Satellites and Drones on critical Intelligence sequence plants, it can precede a scenario on global levels [20].

5. Novel Approaches to Cybersecurity

Zero trust, developed in the early 2000s, is a novel approach in cybersecurity that ensures secure environments in today's perimeter-less architectures. The core of the zero trust model is the stance of "never trust, always verify." Unlike the traditional approach that treats inside users as trusted, the zero trust concept treats any activity on the network as untrusted and scrutinizes all traffic regardless of origin, each action taken by each user is verified and monitored. Implementing zero trust protects against insider threats and lateral movement exploits, preventing the misuse of privileged user access and halting malware propagation from a single incident. Commonly, a zero trust security architecture combines user identity verification, device trustability evaluation, network segmentation, micro-segmentation, granular access controls, telemetry-based analysis, and policies provisioning.

Cyber deception, also referred to as "a cybersecurity mechanism that purposely injects false information to mislead and manipulate an attacker's decision making," is also an emerging novel proactive approach. Cyber deception purposes to mislead attack planning and make any attack less effective.

5.1 Zero Trust Architecture

In adopting the zero trust architecture, an organization is essentially agreeing to the following principles: no one, not even an internal network user, is trusted by default; trust is based on identity verification, device health indicators, and access levels; access is granted on a least-privilege basis; all access requests are dynamically reassessed and logged; activity is monitored, and risks are denied by automated defenses [19]. While the zero trust architecture is beneficial to an organization, it is important to also consider the associated challenges and risks. Some organizations may not have the personnel, budgets, or skills to implement the zero trust architecture. Implementing a zero trust architecture will incur costs related to slowing down the

organization during the transition period, the need for new technologies, and professional development. While it is hoped that the overhead incurred by the zero trust architecture will be outweighed by the increase in security, such measures connected with hoping for the future introduce risk 21.

As with any security architecture, there are risks to the zero trust architecture. Because the zero trust architecture entails a significant technical infrastructure restructuring, any successful compromise of the newly structured architecture could expose a lot of sensitive data or disrupt critical business functions. One inherent characteristic of data breaches is that they go unnoticed sometimes for years. During this period, threat actors could penetrate networks further, gain inside access, develop very sophisticated attack operations, and introduce powerful attack tools. Even if there is a cyberattack, it can be reckless to attempt to retaliate lest the zero trust architecture, which is already fragile, become even more vulnerable, especially if other states or state actors are involved. A successful compromise of a zero trust architecture could be catastrophic for organizations such as banks and other financial institutions.

5.2 Deception Technologies

With the relentless onslaught of sophisticated cyberattacks on enterprises worldwide, traditional signature-based and heuristics detection systems, such as antivirus software, are unable to cope with advanced threats. Deception has emerged as a new line of defense in addition to traditional detection, prevention, and recovery approaches 22. Deception technologies involve manipulation of the beliefs of threat actors to alter their decision-making process through the design of deceptive information, systems, and environments. These technologies can be employed to counteract a diverse range of criminal activities online, including fraudulent email messages, online scams, hacking attempts on enterprises, industrial espionages, and many other intrusions of privacy and manipulations of beliefs [20].

Deception technologies are not necessarily effective against all attackers online, especially if they are designed to be effective against social engineering attacks, spamming, attack of opportunism, or multi-lateral collusion. On the other hand, these strategies are also easy to implement and have been successfully tested in prior experiments. With the advancement of information technologies supporting the creation of decoys, simulations, and the injection of fake information on the Internet, defenders can leverage these innovative strategies to outmaneuver threat actors without violating ethical or legal norms.

6. Technological Innovations in Cybersecurity

Technological innovations have provided novel tools against cybersecurity threats. Blockchain, a decentralized digital ledger technology, has garnered attention due to its potential for providing security in various applications. It makes it possible to create a tamper-proof record of events over the internet, which was previously impossible with conventional technologies. Internet security issues stem from reliance on a central authority. In a blockchain network, nodes are equal and are responsible for tracking the transactions [21]. Cryptography has been the backbone of security for decades, and its growing need in the computing sector has led to interest in quantum computing. Quantum cryptography aims to use quantum mechanics to enhance the transmission sides' currently low power in finding the holography of an area of space. The proposed applications of quantum cryptography in cybersecurity show its potential [22].

Numerous attempts have been made since blockchain's inception to disrupt it and render it useless. Some of these attempts exploit the infrastructure's shortcomings, while others take advantage of human stupidity. Think tanks have also proposed designs to counter these attacks since the concept was put forth in 2008. It is vital to understand the blockchain architecture and its usage to understand the attacks on it. A comprehensive survey enumerating all recorded attacks using recent examples has not been proposed yet. There are different consensus protocols, types of chains, and mechanisms that inspired new attack styles. This paper will provide a detailed discussion of these attacks, the vulnerable points, and countermeasures developed.

6.1 Blockchain for Security

Blockchain is being increasingly utilized for security purposes with various use cases. Network security, IoT security, cybercrime investigation, DDoS prevention, data provenance, and wireless security are among the key areas in the field of cybersecurity where blockchain technologies are applied [22]. Particularly, the advent of cloud computing and storage has turned out to be a double-edged sword for cybersecurity, whilst providing secure data protection services, on the other hand, it has raised some new security concerns. Several service-as-a-software (SaaS) data protection schemes using blockchain technology are proposed to protect against data integrity violation, data access control violation, and illegal data sharing. On a broader scope, cyber-attacks are studied in various dimensions, including detection, recovery, planning, attribution, effect prediction, and evolution analysis. Several solutions on network defense, deep learning, game theory, and Artificial Intelligence (AI) are proposed for a fair game between attack and defense [23].

Still, despite the wide range of use cases outlined for blockchain technologies in cybersecurity applications, these technologies are not completely free from drawbacks. For example, although public key infrastructure (PKI) addresses the key leakage problem to some extent, it has assumed that the conventional traditional PKI system to be foolproof. Additionally, smart contract-enabled legislative aspects of law enforcement raise concerns over security, efficiency,

feasibility, lower cost, and effectiveness trade-offs among societal actors. Moreover, the probabilistic nature of blockchain and related cryptographic mechanisms could not achieve a certain effectiveness, viability, and long-term sustainability in very large or extremely sensitive governmental cybersecurity areas. Similarly, challenges are discussed on a more macroscopic and strategic level. In particular, the topological and architectural threats of next-generation cyber-attacks on offensive capabilities, cyber-weapons, and the potential role of blockchain technology to build cyber-deterrents are outlined.

6.2 Quantum Cryptography

In recent years, quantum cryptography has gained significant traction as a potential solution to a major concern in security: how to communicate securely with no risk of eavesdropping [24]. As a fundamental property of quantum mechanics, the uncertainty of observables guarantees that if an eavesdropper tries to obtain information on a quantum system, its effect can be easily detected. As such, there is great interest in combining cryptography and quantum mechanics in such a way that one can take advantage of the laws of physics to provide a solid foundation for the security of a cryptographic system. This has led to the design of a set of protocols using quantum mechanics to solve cryptographic tasks using quantum channels [25].

The most widely known and studied example is quantum key distribution. A recent paper presented a novel approach to increasing the efficiency of this protocol and making it suitable for the current technology gap (90% efficiency for short distances) with a realistic testbed to be implemented: pseudo Bell state measurement [26]. This approach analyzes a design based on the transmission of Bell states through noisy quantum channels.

7. Human Factors in Cybersecurity

The role of human factors as systems and technologies become more advanced and automated, human factors issues start to dominate the design. Understanding how a system fits into the organizational, social, cultural, and technological context in which it will be used is critical to improving the system design. It is also worldly recognized that mistakes, errors, and unwanted actions originate from a breakdown in the 'sociotechnical' system used in the context [27]. A breakdown can be the consequence of poor design, badly implemented changes, and/or problematic underlying organizational and social factors.

As the world becomes more technologically advanced and interconnected, people rely on computers to perform essential activities. They expect that these computers work correctly: processing the desired data, providing adequate and trusted user-interface presentation, preventing unwanted consequences, and safeguarding all needed confidentiality, integrity, and availability properties [28]. The role of people, however, remains key in the effective operation of information and computer systems. Specifically, many contemporary cyberspace vulnerabilities are the direct (or indirect) consequence of unwanted actions by computer users. Even though security issues that arise from these actions are deeply rooted in the design of the technological systems and the organization and distribution of social powers, many cybersecurity measures exclusively focus on providing technological solutions like firewalls, antivirus software, and other monitoring and filtering systems.

7.1 Social Engineering Awareness

The development of cybercrime and its consequences has had a serious impact on social engineering and, in particular, phishing attacks. Phishing attacks are viewed as a dangerous and increasing threat, which can take many forms of acquisition. They include an array of malware to infiltrate computers or credential harvesting. Some of the most common of such attacks are typed-in attacks, where the target is tricked to enter the requested data into fake Webpages, and Pop-Up attacks where messages inform about threats to the target computer and trick the victim into running an executable file.

People tend to be unaware of phishing attacks and most often take the documents for the original one, which contributes to the attack's serious consequences [29]. As a comparison, physical thefts and computer break-ins are easily identifiable as high-risk situations. However, there are methods to lower the risk of successful phishing attempts such as enhanced anti-phishing software. Phishing is a criminal method that seeks to gain personal and financial details from the user and create damages for companies. The relation of personal damages and the security of the company results in increased risks for the user and suggests that more attention should be given to the need for user awareness regarding phishing. The level of social engineering knowledge can still be used as a security countermeasure affecting the number of occurrences related to such attacks and the damage from them.

7.2 Insider Threats

Every organization is at risk for insider threats when individuals with authorized access to sensitive information turn malicious for various reasons. Trust in individuals and allowing them access to company information is essential to an organization. However, it is imperative to ensure that trust is not misplaced. Security breaches by trusted individuals in organizations, both intentionally and inadvertently, are called insider threats [30]. Current security measures are not designed to detect insider threats and the culture of blame within organizations stifles the reporting of security violations. An organization can be proactive in identifying suspicious behavior before an incident occurs by educating individuals on how to spot the behaviors of concern. Education also broadens the focus on security and information assurance from the IT department to the entire organization. It instills accountability and

responsibility for actions taken across the entire organization. Diagnostic tools can also be employed to aid in detecting and investigating malicious insider behavior.

An insider threat is a security risk that comes from trusted individuals such as employees or business partners who have inside information concerning the organization's security practices [31]. These threats have been the main issue for both national security and global business issues leading to great financial losses and the downfall of some prominent multinational companies. Technology advancement with E-Payment boosted globally to more than 8 trillion dollars in 2018, thus making it critical for understanding that along with these advancements in the software systems, cyber trouble also comes in. In most cases, malicious activity takes weeks or longer to detect, thus allowing an intruder ample time to steal or destroy the assets of an organization. Most of the cases are still unidentified such as the Bangladesh robbery case where over 81 million dollars were withdrawn. Security is tested by the most trustworthy individual who has free access to all data and resources of an organization which is why a vast majority of cyber-attacks are caused by trusted users such as employees or ex-employees. On average, insider threat handling costs around 8 million dollars to the organization!

8. Regulatory and Compliance Frameworks

Regulatory compliance remains a significant issue, with ongoing need for clarity about what is expected across industries and jurisdictions, particularly for emerging tech. The ubiquity of Edge AI, generative AI, and other machine-learning systems will create challenges for compliance and assure adherence to organizational policies, data governance, and local laws. Developing Assurance and Compliance Platforms capable of real-time oversight of compliance, risk, and performance continues to be a very high priority for many organizations, and more research in this space would represent a sensible investment in most transaction domains [32].

Given the growing prevalence of cross-border data sharing, the sharing of personal data is one of the main determining factors in choosing where to put organizations and their business, especially regarding personal data. This is likely to continue and become an important public interest topic. In maintaining a free-flowing data environment, it is essential to consider breaches of privacy and data abuse, thereby determining further lawful ways to share data as broadly as possible. There are a few alternatives to the strict applicability of general regulations like the GDPR that are also still in their infancy, such as a more blend and mixed system of consent measures and legal standards such as de-identification (anonymization) and public good exceptions, also potentially addressed in the PDPA. However, too broad an applicability may thwart data sharing [33].

8.1 GDPR and Data Protection

In the 21st century, the rapid growth of information technology and communication systems has brought about a sharp increase of personal data processing across the globe. During this time, the data leak incidents happened in many organizations that resulted in heavy loss of personal data. To encounter such incidents, a new and updated data protection regulation was drafted by the European Union (EU), known as the "General Data Protection Regulation" (GDPR). The data protection laws made by the EU always focused on "the accompanying right to privacy" and hence, the pejorative description of privacy resulted in the concept of data protection 34. The data protection regulation would require addressing these concerns and affect many cybersecurity practices.

The GDPR has a considerably broader scope of applicability over its predecessor directive compared to most data protection laws around the world where the territorial scope is typically quite limited. Inconsistency with the current data protection laws around the world in relation to the "right to portability", "right to erasure", and "guarantee of privacy by design" also need to be addressed. The data controllers/processors would be completely responsible for complying with the legal requirements. Hence, processed personal data are required to be in an intelligible form to the data subject unless the data concerns, etc. [33]. This huge new sector would require extra labor forces and intense workforce training in compliance with laws already there and also the upcoming GDPR. Whether enough human resources would be available to meet such requirements can easily be imagined [34].

8.2 Industry-Specific Regulations

Presently, many industries that continuously handle sensitive information and provide critical services, such as financial, energy and health, are subject to industry-specific regulations. Cybersecurity regulations vary widely across industries and countries, which presents compliance problems for companies that operate in more than one industry or country. Generally, regulations can be classified as mandate-based compliance, which often results in a compliance checklist approach, and logic-based compliance, which require entities to demonstrate the reasoning behind policy decisions [35]. The strength of logic-based compliance is its adaptability to a wide range of internal and external contexts. However, such contextual depth requires comprehensiveness of compliance reporting which is a challenge for many organizations with complex enterprise architecture, especially those with legacy systems. In this case, compliance becomes an enterprise architecture problem [36].

In general, there are three common patterns of cybersecurity regulations. Firstly, some regulations are industry-specific, affecting only certain industries. For example, the Gramm-Leach-Bliley Act (GLBA) applies to financial services companies and imposes certain requirements respecting the protection of consumer

financial information. Such a pattern typically results in compliance problems for companies that operate in more than one industry. Secondly, compliance requirement lists are different for large and small entities, or for public and private entities. For example, Section 404 of the Sarbanes-Oxley Act and similar regulations typically apply only to publicly traded corporations. Such a pattern also generates compliance problems for companies that operate in both public and private domains. Thirdly, certain regulations can have global applications. For example, the Payment Card Industry Data Security Standard (PCI DSS) and the Hague Convention on Cybercrime can affect organizations in many countries around the world.

9. Cybersecurity in Critical Infrastructure

The development of cybersecurity measures for critical infrastructure, construction, and energy management software is explored. The attack on energy management software developed by Schneider Electric is described, leading to concerns about data theft, infrastructure execution issues, and energy service consumption. A cybersecurity model is proposed, focusing on prevention, interventions, and management of post-attack consequences. Preventive measures involve employee periodic training, network attack simulations, and end-user program installation. Leaving workstations unmonitored when employees are absent is investigated. The adequacy of proposed preventive measures is evaluated, and recommendations for enhancement are provided [37].

Specific vulnerabilities and possible attacks in two essential areas of public life that have not been addressed adequately before or have been poorly covered are studied. Many advancements in cybersecurity are concerned with improving or implementing general security measures; however, specific ones have not concerned specific vulnerabilities and possible attacks [38]. Typical ones are introduced into focus, particularly those related to the energy sector and the healthcare industry. The emergence of these vulnerabilities and how they can become evident are discussed, along with measures that should be taken before they happen.

9.1 Energy Sector Security

Long-standing guidelines defining the intent and scope of physical security have survived scrutiny and adaptation better than equivalently meaningful terms within the context of information assurance. The U.S. government worried about the impact of computer security on economic competitiveness as far back as 1977. In the early 1980s, CRT terminals, minicomputers, stand-alone personal computers, and SNA networks burgeoned with virtually no security. Software-based intelligence was required to identify and monitor politically or economically destabilizing events in the computer information system. Concerns arose that attackers could be highly motivated, highly capable, and/or can exploit the trivial nature of vulnerabilities. Political and technical criteria were defined for threats posed to commercial firms by governments, organized crime, and anarchists. Data-based intelligence systems were called for. In response to this troubled and troubling world, growing investments in CII hardened the most expensive and most important systems, and invested in a performance-honored improvement, secure enclaves.

The implications for energy sector security are far reaching. Potential vulnerabilities arise between and within electricity and oil and gas infrastructures because of new technologies, processes, and business models. Compliance with end-to-end, all-hazards, prevention through design (PtD), and metrics for risk-based assessments will be required. The energy sector is overwhelmingly privately owned and operated, raising contentious and complicated issues regarding national sovereignty, transparency, and regulation. Current approaches to cybersecurity have trouble addressing continued rapid attacks and growth of vulnerabilities. Embedded systems will soon dominate all other systems. This might be the ‘new-paper’ moment for information systems, but many intimately familiar with CII have spent careers trying to avoid relying on paper underestimation of risks. Just because ‘its hard and costly’, do not expect the energy sector to adopt protective strategies like those outlined by power grid experts [39].

9.2 Healthcare Industry Vulnerabilities

There is an increase in cybersecurity threats to healthcare, as due to digitization, device connectivity, and interaction with recent technologies, such as Artificial Intelligence (AI), healthcare systems are found exposed to cyberspace and vulnerabilities. The purpose of this paper is to identify cycle trends, types, and ways forward to limit cyber-incidents in healthcare. Today’s healthcare data is potentially sensitive, private, and confidential. A lot of services are now based on the Internet, and there is an increase in medical instrument connectivity with networks, devices, and the Internet as “smart” devices. A new market is evolving, such as remote patient management, diagnostics, treatment, and tele-health services 40.

10. International Collaboration in Cybersecurity

As cyber threats become increasingly sophisticated and pervasive, the need for international collaboration in cybersecurity has grown. Many organizations and initiatives have been established to facilitate information sharing, policy coordination, and joint research efforts [41]. Public-private partnership initiatives have been launched in several countries, including the European Union and China, which encourage businesses to share cyber threat information with other organizations in the same sector or geographic area. The European Union’s Public-Private Partnership for Resilience Cybersecurity (EP3R) is one such initiative that

seeks to bring together security and Information and Communication Technology (ICT) stakeholders to meet challenges and share knowledge on risks and best practices [42].

The technical community, including academic research institutions and security companies, has also engaged in extensive information sharing projects focused on cyber threat detection and mitigation. The Platform for European Security Research – EUREKA (EUSec) project provides a good example of ongoing industrial, government, and academic know-how exchanges in cybersecurity via common research initiatives. Initiated in 2010, this flagship project aims to fix Europe's security research and innovation gap with third countries, including the USA, Canada, and Japan [43].

10.1 Information Sharing Initiatives

The challenges posed by these shared cyber threats must be met with collaborative answers. Many organizations are considering information sharing initiatives to better address and mitigate the increasing scale, sophistication, and impact of these global threats [44]. The pursuit of improved security and resilience in network systems and infrastructures has led to greater recognition of the role that information sharing between trusted partners can play in preemptively identifying and countering advanced attacks, as well as understanding and recovering from disruptions.

The usefulness of a more collaborative approach has been increasingly recognized in many communities facing shared risks. Growing awareness of the need for an "ecosystem" approach has led to the formation of these groups in a broad range of sectors (e.g. telecommunications, financial services, oil and gas, electric power, and others) [45]. Addressing new threats as they emerge — such as internet worms, denial of service attacks, and espionage-based attacks - is anticipated to be much more effective when multiple organizations work together to share information. As a first step, there must be a basic understanding of the information requirements and other resource requirements for collaboration. The information security community must investigate what information actually needs to be shared to accomplish desired collaborative goals, such as detection of class attacks, protection against certain types of attacks, or mitigation of a specific observed attack.

10.2 Joint Research Efforts

In recent years, targeted attacks against networks, operating systems, and applications have increased dramatically. Therefore, defense mechanisms need to be developed for security flaws in both software and hardware along cybersecurity pipelines, including vulnerability analysis and mitigation and software free of known vulnerabilities 2. In addition, when it comes to covert and overt attacks on free software distributions and libraries, significant gaps exist in the utilization of sophisticated threat models. However, in a cascade of recursive attacks, malware, including worm-style infections, superinfecting complex and sophisticated homogenous networks, may evade the majority of mitigation approaches and exploitation prevention technologies. The significance of economically viable risk assessment methods conducive to large-scale simulation modeling, investigation of cyber-attacks on critical infrastructure, and development of powerful algorithms to turn the results into defense policy is pointed out.

Joint efforts in cybersecurity have only recently gained momentum, despite a long-standing tradition of collaboration in defense and security research across Europe. National governments as well as the European Union are prioritizing the protection of public goods. In this context, cybersecurity takes center stage in addressing European infrastructural weaknesses comprising and critically depending on public and private online systems, such as banking, energy networks, public transportation, and telecommunications [43]. Consequently, the significance of combined endeavors has been ever more emphasized in developing innovative solutions and strategies to act and react against evolving threats.

11. Future Directions and Challenges

Current advancements in Generation 6 Cybersecurity offer enormous perspectives aimed at maintaining current systems or developing new approaches. There are several technologies and approaches with the potential to enormously boost current most prevalent systems and maintain the core of already established systems as a strong basis. Artificial Intelligence (AI) is a very powerful technology that has started being effectively incorporated into the cyber threat scope. It can reverse or outturn the above-discussed effects of cyber technologies in favor of proactive development in the fight against cyber threats 14. AI-based systems can be created and implemented to radically bolster current and already established means of defense or create new ones that might otherwise have remained unfeasible. Such systems would monitor all network traffic and activity, identify and analyze patterns of potential vulnerabilities and risks and forward or even autonomously execute responses to reinforce security. Furthermore, the very nature of risk and threat perception could be transformed, offering entirely new perspectives on analyzing already developed systems. The discriminatory potential of AI could identify weaknesses of classical logic or counter intuitiveness and render them meaningless.

Like other technological advances, this one comes with limitations and risks as well. One of the challenges is the unpredictability of AI. The lack of understanding of how it actually functions often fuels claims and fears of runaway AI. Such scenarios cite the possibility that an AI response or action may deviate from its intended goals. This could be the case with black-box algorithm designs or AI implemented systems that were not properly trained. Development of super-intelligent AI has also been cited as

having the potential of doing more harm than good and turning the benign AI against its creators if devised by malicious actors to protect their interests. 17 also identifies further negative applications broadening the scope of risk exposure at least to the extent of suggesting additional moral studies. AI can be used to create deep fakes with a twist on the effect of cyber warfare that can serve as a powerful disinformation weapon used for the benefit of companies or states.

11.1 Artificial Intelligence in Cybersecurity

The cybersecurity landscape is rapidly evolving. New and emerging technologies are shaping the landscape by creating new opportunities for individuals and organizations to increase safety as well as new vulnerabilities that must be addressed. Artificial intelligence (AI), machine learning (ML), and automation are among the technologies reshaping the defensive and offensive security space. As a consequence, highly sophisticated cybersecurity threats and attacks that are capable of impacting critical infrastructure and national security are expected to increase in frequency and sophistication. Against this backdrop, a discussion of AI and its role in shaping the future of cybersecurity is pertinent 14.

Cybersecurity has emerged as the most daunting problem over the last decade. Over the years, individuals and organizations have invested significant resources in preventive mechanisms to ensure safety and security. The evolution of the digital era has acted as an enabler for individuals and organizations to increase productivity and efficiency. However, the advent of this technology has created numerous vulnerabilities and concerns. Interconnected and technological systems of today expose organizations to an increasing number of complex cybersecurity attacks. These attacks are sophisticated and are influenced by factors such as increasing knowledge, access to resources, and awareness among cybersecurity adversaries. These developments have required organizations to state-of-the-art and new technologies to ensure cybersecurity [46].

11.2 Ethical Considerations

Virtually every aspect of modern life depends on interconnected systems or networks of systems, whose design involves both technical and social considerations. The constitutional design of such systems can give rise to moral and ethical dilemmas. An ongoing moral and ethical debate flows from a wide range of ensuring technologies used within the pursuit of cyber-security. This wide range includes, but is not limited to, ethical hack(ing) techniques, cyborg rights, artificial intelligence, de-anonymisation and behavioral profiling technologies [47].

Such dilemmas can be construed as both an understanding of cyber-security socio-technical issues as well as a critical examination of cyber-security design. In the latter case, cyber-security distinction can be understood in the sense of a design concern, which demands an examination of moral and ethical issues of any given technical resolution. The design consideration perspective allows a critical investigation into the social and theoretical constructs underpinning the moral and ethical questions. Inquiring mind into moral and ethical controversies might lead to ways of understanding how socio-technical cyber-security designs operate and what social constitutions of risk and safety they produce. Empirical studies involving moral and ethical deliberations about the ongoing design of cyber-security technologies could allow interests and concerns to be articulated that might otherwise not come to the fore. Such investigations would also allow a public understanding of the social and theoretical considerations shaping the design of cyber-security on the broader domain level [48].

12. Conclusion

Emerging technologies have brought new cybersecurity threats. As a result, cybersecurity approaches should adjust to industry needs and the new level of vulnerabilities 1. The examination of cybersecurity approaches based on novel technologies affords a view of the future trends on an industry level. Moreover, the outlook on emerging vulnerabilities in cybersecurity in future technological advancements gives a broader understanding of general implications on the industry and the whole internet.

While technological advancement is one of the main drivers of cybersecurity threats, it instigated proactive approaches to help defend against new vulnerabilities. Network anomaly detection methods and employment of AI in cybersecurity will more likely continue in the future as necessary standards and requirements to combat against the sophistication of new cyber threats. Moreover, overall interest in the reliability of the Internet of Things and associated devices will stimulate further legislation and implementation of security protocols for the improvement of public safety and quality of life. Addressing these issues will also make it easier to mitigate against other threats that arise from using current technological capabilities to an extreme. Overall, addressing considerations for cybersecurity in emerging technological advancements will help sustain global digitalization.

12.1 Summary of Key Findings

Cyber security threats pose potential danger to national security, including the government and military, as well as individuals, corporations, and other organizations. The emergence of the Internet has contributed to this phenomenon. The rise of government-owned infrastructures has created the need for cyber security analysis for individual state control and sovereignty. The rise of the so-called cyber weapons and preemptive military cyber-attacks has fundamentally changed and threatened the diplomatic aspect of state sovereignty. To help comprehend the threat, the cyber security landscape in the context of the threat

along with potential dangerous scenarios are mapped, accordingly 4.

By comparing case studies of cyber security threats against corporations, it is explained how cyber security threats outside of government control and sovereignty become commercialized and used to execute corporate espionage. The security capability between large corporations and small to medium corporation was compared, revealing a steep divergence in capability. This indicates a shift into a new paradigm where traditional logic of proactive corporate espionage has been overturned and turned on its head, where small to medium corporations with high level of IP knowledge would be targeted. The necessity of conducting vulnerability analysis is proposed, a comprehensive and sophisticated method of detecting threat and vulnerability by scenario construction is presented 1.

12.2 Implications for the Field

The implications for the field of cybersecurity are presented. The purpose of this section is to consider what impact the advancements and challenges in cybersecurity discussed above would have on cyber security in general and how it would change the way cyber security is spent, the way research is directed and how crucial issues are approached concerning the future in which the discussion is framed.

The implications for the field in numerous facets of cybersecurity, for example, operating systems implementation and application decisions made to meet the security requirements of such applications, are considered 3. Consideration is then given to the implications for the futures of the organization, the community and the state in the extent to which they would remain removing the issues associated with emerging examples of crime and illegality. Finally, an attempt is made to consider what the implications for the social, cultural, ethical and political context in which the technologies are situated [49].

References

[1] T. M. Kelly, "Who's In and Who's Out?: What's Important in the Cyber World?," Honors Project, La Salle University Digital Commons, 2016.

[2] K. Ishaq and S. Fareed, "Mitigation Techniques for Cyber Attacks: A Systematic Mapping Study," *arXiv:2308.13587*, p. 19, 2023.

[3] S. Alam, *Cybersecurity: Past, present and future*. arXiv:2207.01227, 2022, p. 123.

[4] J. Scott, "Phobic Cartography: Human-Centred, Communicative Analysis of the Cyber-Threat Landscape," *Journal of Information Warfare*, vol. 16, no. 4, pp. 93-112, 2017.

[5] J. M. Borky and T. H. Bradley, "Protecting information with cybersecurity," in *Effective Model-Based Systems Engineering*: Springer, Cham, 2019, ch. 10, pp. 345-404.

[6] K. Sadhukhan, R. A. Mallari, and T. Yadav, "Cyber Attack Thread: A control-flow based approach to deconstruct and mitigate cyber threats," in *2015 International Conference on Computing and Network Communications (CoCoNet)*, Trivandrum, India, 2015: IEEE, pp. 170-178, doi: https://doi.org/10.1109/CoCoNet.2015.7411183

[7] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-Attack Penetration Test and Vulnerability Analysis," *International Journal of Online Engineering*, vol. 13, no. 1, pp. 125-132, 2017, doi: https://doi.org/10.3991/ijoe.v13i01.6407

[8] M. S. Weiss, "Network defense: The attacks of today and how can we improve?," MSc Thesis, Rochester Institute of Technology, 2009.

[9] E. Schrom *et al.*, "Challenges in cybersecurity: Lessons from biological defense systems," *Mathematical Biosciences*, vol. 362, p. 109024, 2023, doi: https://doi.org/10.1016/j.mbs.2023.109024

[10] B. O. Lawal and J. O. Okesola, "Managing Network Security with Snort Open Source Intrusion Detection Tools," in *International Conference on Science, Technology, Education, Arts, Management and Social Sciences*, Ado-Ekiti, Nigeria, 2014, pp. 471-482.

[11] H. Friji, I. Mavromatis, A. Sanchez-Mompo, P. Carnelli, A. Olivereau, and A. Khan, "Multi-stage Attack Detection and Prediction Using Graph Neural Networks: An IoT Feasibility Study," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Exeter, United Kingdom, 2023: IEEE, pp. 620-627, doi: https://doi.org/10.1109/TrustCom60117.2023.00095

[12] U. Mishra, "How do Viruses Attack Anti-Virus Programs," arXiv:1307.5420, 2013.

[13] P. Singhal and N. Raul, "Malware detection module using machine learning algorithms to assist in centralized security in enterprise networks," *arXiv:1205.3062*, p. 7, 2012.

[14] S. Bernardez Molina, P. Nespoli, and F. Gómez Mármol, "Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision," *e-prints arXiv:2312.06229* pp. 1-34, 2023, doi: https://ui.adsabs.harvard.edu/link_gateway/2023arXiv231206229B/doi:10.48550/arXiv.2312.06229

[15] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "IoT network security: requirements, threats, and countermeasures," *arXiv:2008.09339*, pp. 1-13, 2020.

[16] N. Singh, R. Buyya, and H. Kim, "IoT in the Cloud: Exploring Security Challenges and Mitigations for a Connected World," *arXiv:2402.00356*, pp. 1-27, 2024.

[17] M. Schmitt, "Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection," *Journal of Industrial Information Integration*, vol. 36, p. 100520, 2023, doi: https://doi.org/10.1016/j.jii.2023.100520

[18] B. Hallaq, T. Somer, A.-M. Osula, K. Ngo, and T. Mitchener-Nissen, "Artificial intelligence within the military domain and cyber warfare," in *ECCWS 2017*

16th European Conference on Cyber Warfare and Security, 2017, pp. 153-157.
[19] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: A brief survey," *Entropy*, vol. 25, no. 12, p. 1595, 2023, doi: https://doi.org/10.3390/e25121595
[20] Z. Lu, C. Wang, and S. Zhao, "Cyber deception for computer and network security: Survey and challenges," *arXiv:2007.14497*, pp. 1-7, 2020.
[21] K. Strandell and S. Mittal, "Risks to zero trust in a federated mission partner environment," *The Cyber Defense Review*, vol. 8, no. 3, pp. 89-98, 2023.
[22] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. Kamhoua, and M. P. Singh, "Game-theoretic and machine learning-based approaches for defensive deception: A survey," *arXiv:2101.10121*, p. 37, 2021.
[23] B. Saha, M. M. Hasan, N. Anjum, S. Tahora, A. Siddika, and H. Shahriar, "Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures," *arXiv:2306.11884*, pp. 1-29, 2023, doi: https://doi.org/10.48550/arXiv.2306.11884
[24] M. Jobair Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities," *e-prints arXiv:2207.03534* p. 8, 2022, doi: https://ui.adsabs.harvard.edu/link_gateway/2022arXiv220703534J/doi:10.48550/arXiv.2207.03534
[25] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147-156, 2020, doi: https://doi.org/10.1016/j.dcan.2019.01.005
[26] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," *arXiv:2404.10659*, pp. 1-25, 2024, doi: https://doi.org/10.48550/arXiv.2404.10659
[27] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig, "Human factors in security research: Lessons learned from 2008-2018," *arXiv:2103.13287*, p. 23, 2021, doi: https://doi.org/10.48550/arXiv.2103.13287
[28] R. Montanez Rodriguez, E. Golob, and S. Xu, "Human Cognition through the Lens of Social Engineering Cyberattacks," *e-prints arXiv:2007.04932* p. 24, 2020, doi: https://ui.adsabs.harvard.edu/link_gateway/2020arXiv200704932M/doi:10.48550/arXiv.2007.04932
[29] O. S. Salem, "An Integrated Intelligent Approach to Enhance the Security Control of IT Systems. A Proactive Approach to Security Control Using Artificial Fuzzy Logic to Strengthen the Authentication Process and Reduce the Risk of Phishing," PhD Thesis, University of Bradford, 2012.
[30] J. L. Wunderlich, "The insider threat," MSc Thesis, Regis University, 2011.
[31] A. P. Singh and A. Sharma, "A systematic literature review on insider threats," *arXiv:2212.05347*, p. 9, 2022, doi: https://doi.org/10.48550/arXiv.2212.05347
[32] T. R. McIntosh *et al.*, "From cobit to iso 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," *Computers & Security*, vol. 144, p. 103964, 2024, doi: https://doi.org/10.1016/j.cose.2024.103964
[33] A. Albakri, E. Boiten, and R. De Lemos, "Sharing cyber threat intelligence under the general data protection regulation," in *Privacy Technologies and Policy*, 2019: Springer, pp. 28-41, doi: https://doi.org/10.1007/978-3-030-21752-5_3
[34] A. ALibeigi, A. B. Munir, M. E. Karim, and A. Asemi, "Towards standard information privacy, innovations of the new general data protection regulation," *Library Philosophy and Practice*, vol. 2840, p. 20, 2019.
[35] E. Haber and T. Zarsky, "Cybersecurity for infrastructure: a critical analysis," *Florida State University Law Review*, vol. 44, p. 515, 2016.
[36] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Computer Law & Security Review*, vol. 34, no. 3, pp. 450-466, 2018, doi: https://doi.org/10.1016/j.clsr.2017.12.004
[37] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship and sustainability Issues*, vol. 4, no. 4, pp. 559-573, 2017, doi: http://doi.org/10.9770/jesi.2017.4.4(12)
[38] F. A. Batarseh, "Cybersecurity Law: Legal Jurisdiction and Authority," *arXiv:2206.09465*, pp. 1-22, 2022, doi: https://doi.org/10.48550/arXiv.2206.09465
[39] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, 2021, doi: https://doi.org/10.3390/s21186225
[40] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48-52, 2018, doi: https://doi.org/10.1016/j.maturitas.2018.04.008
[41] K. Lampropoulos *et al.*, *White paper on cybersecurity in the healthcare sector. The HEIR solution*. arXiv:2310.10139, 2023, p. 70.
[42] M. A. Ben Naseir, H. Dogan, E. Apeh, C. Richardson, and R. Ali, "Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study," in *New Knowledge in Information Systems and Technologies*, 2019: Springer, Cham, pp. 373-382, doi: https://doi.org/10.1007/978-3-030-16181-1_35
[43] D. P. Fidler, R. Pregent, and A. Vandurme, "NATO, Cyber defense, and international law," *St. John's Journal of International and Comparative Law*, vol. 4, p. 1, 2013.
[44] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana, "Shall we collaborate? A model to analyse the benefits of information sharing," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, Vienna, Austria, 2016: Association for Computing Machinery, pp. 15-24, doi: https://doi.org/10.1145/2994539.2994543
[45] E. M. Sedenberg and J. X. Dempsey, "Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs," *arXiv:1805.12266*, pp. 1-27, 2018, doi: https://doi.org/10.48550/arXiv.1805.12266

[46] N. Dhir, H. Hoeltgebaum, N. Adams, M. Briers, A. Burke, and P. Jones, "Prospective artificial intelligence approaches for active cyber defence," *arXiv:2104.09981*, pp. 1-5, 2021, doi: https://doi.org/10.48550/arXiv.2104.09981

[47] X.-L. Palmer, L. Potter, and S. Karahan, "On the emerging area of biocybersecurity and relevant considerations," in *Advances in Information and Communication*, 2020: Springer, pp. 873-881, doi: https://doi.org/10.1007/978-3-030-39442-4_66

[48] G. Lorenzini, D. M. Shaw, and B. S. Elger, "It takes a pirate to know one: ethical hackers for healthcare cybersecurity," *BMC Medical Ethics*, vol. 23, p. 131, 2022, doi: https://doi.org/10.1186/s12910-022-00872-y

[49] M. Williams, L. Axon, J. R. Nurse, and S. Creese, "Future scenarios and challenges for security and privacy," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Bologna, Italy, 2016: IEEE, pp. 1-6, doi: https://doi.org/10.1109/RTSI.2016.7740625

How to cite this article

A. A. Hammad, H. M. Saleh, and M. F. Alomari, "Advancements in Cybersecurity: Novel Approaches to Protecting Against Emerging Threats and Vulnerabilities," *CyberSystem Journal*, vol. 1, no. 1, pp. 9-22, 2024. doi: 10.57238/r15e5074

Access this article online