Shairoze *et al.LGU (IJECI)* 2022

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 6 issue 2 Year 2022

A Review of Cyber Security and Cyber-Attacks – What to Know?

Muhammad Shairoze Malik
School of Electrical engineering and computer Sciences, National University of Science and Technology, Islamabad.

Abstract

In this era, human activities have seen a shift and our majority activities including social, cultural, economic and even governmental and NGOs are being done in the cyberspace, especially during and after the crisis of corona pandemic. Due to this shift in communication culture, many individuals and organizations including governments have to face cyber-attacks. Due to heavy reliance on technology and little awareness, defending against cyber-attacks is very challenging. Cyber attacks are usually conducted with the goal of harming an organization or individual financially or these attacks may also be motivated for political or military purposes. Viruses, malwares, ransomwares, denial-of-service and phishing attacks are some of the examples. To protect themselves, organizations employ variety of strategies to mitigate or prevent the threat of these attacks. To prevent and mitigate cyber-attacks, researchers and professionals have devised a number of techniques. This paper is written to thoroughly study and analyze these various approaches and proposed cybersecurity standards, and also to look into the problems, limitations and strengths of these techniques. Fundamental concepts of cyber-attacks and cyber security are discussed along with the current advancements and upcoming trends in security of cyber space. Such a comprehensive review paper would be highly beneficial.

Keywords: Cyber Security, Cyber-Attacks, Information Technology, Key Management, Emerging Trends

1. Introduction

Internet has become an essential part of our daily lives for the more than two decades now. Due to the technological enhancements and low prices, the internet facility has seen a big boost in its availability, performance and uses. More than 3 billion users are connected to internet now worldwide [1]. Due to e-commerce and other activities, billions of dollars are generated by the global network of internet which has now become a significant portion of global economy [2]. Currently, the majority activities including social, cultural, economic and even governmental and NGOs are being done in the cyberspace [3]. Cyber space has become a center piece in controlling

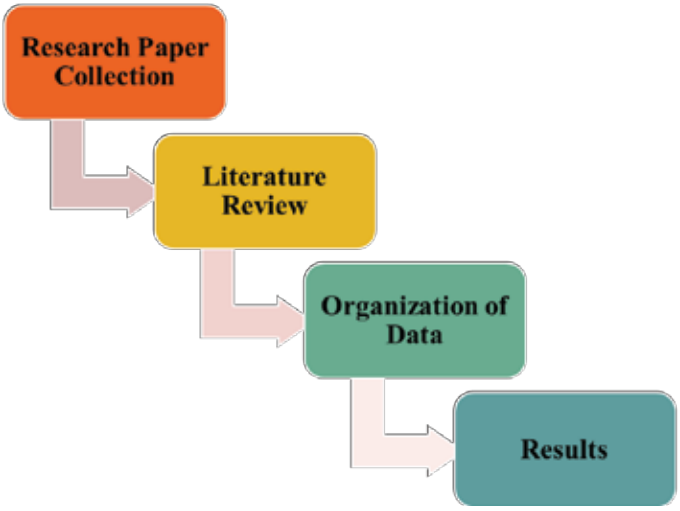
and sharing important and sensitive information around the world [4]. Cyber space has seen a significant increase in activates and financial transactions, through social media and other websites, a significant portion of people's daily life and activities are spent in cyber space as well [5]. A country's GDP (Gross Domestic Product) now has a significant percentage through online companies like e-commerce or freelancing and cyberspace indicators are showing that this percentage is on the rise. These days' cyber space is linked to income and success of a significant portion of people globally [6]. In other words, several components of social life are connected to cyber space and any problem that arise in this space like insecurity or instability will have a direct effect on various areas of social life in real world [7]. All this adds to the problems and challenges for the users and organization which are working in online industry. Low cost to use, anonymity and lack of knowledge about cyber threats have resulted in a rise in cybercrimes either conducted against individuals or organizations by malicious groups or individuals equipped with proper knowledge. Cyber warfare, cyber terrorism, cyber bullying, and cyber espionage are some examples of cybercrimes [8]. All this leads to a very dangerous situation for national security as cybercrimes are not like traditional security threats where the threat actors are usually out in the open [9]. Specialist and analyst have been debating the potential of cyber-attacks on national security for decades [10]. There are numerous incidents of widespread physical and economic damage due to cyber-attacks like an attack on the banking system or virus to disrupt stock market activities or disruption to supply of power by injecting incorrect commands in system or disruption to air traffic control system can cause air accidents, all these cause countries to shut down its operations and lead to security issues [11] [12]. Experts struggle to cope with the cyber-attacks due to a large number of attack vectors across various technologies. It also becomes difficult to enact proper laws and mitigation strategies unless countries have a clear definition of cyber-attacks which are acknowledged by international community [13]. As a result, the question arises [14] as to;

- What constitutes a cyber-attack?
- What its feature are?
- If any attack occurs in cyber space can it be regarded as a crime in its proper definition.

The availability of proper definitions and categorization of cyber-attacks can no doubt help legal fraternity to establish proper laws and punishments. Without a clear picture and lack of knowledge about severity of cyber-attacks, it leads to diversity in interpretations and practices which eventually leads to sometimes contradicting legal results [15] [16]. Therefore, the importance of fundamental knowledge of cyber-attacks, there working and analysis is of paramount importance and it necessitates extensive and continuous research. The foundational knowledge of cyber-attacks is discussed in this paper, followed by an analysis of mitigation techniques and categorization of cyber-attacks. Current definitions are analyzed from the perspective of global specialists and organizations. In the end conclusion of paper is provided.

2. Methodology

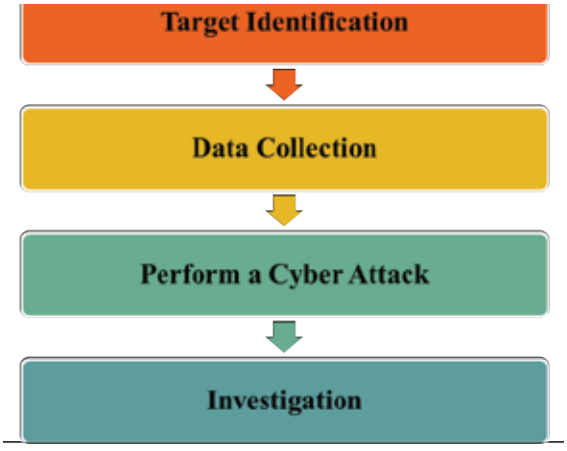
The methodology used in this research paper is explained in the below diagram:



(Figure 1: Methodology)

3. Fundamental Concepts

Cyber assaults are part of a larger context than what is generally referred to as information operations. Electronic warfare, psychology, computer networks, military tricks and security operations, and other major capabilities, combined with special support and related capabilities, are used extensively in information operations to infiltrate, hijack or stop human decision-making [17]. The steps of a cyber-attack can be depicted as shown in Figure 2.



(Figure 2: Anatomy of a Cyber-Attack.)

Computer network operations, according to the USNM cyberspace operations strategy, include attack, defense, and exploit enablement [18]. The latter differs from cyber assaults and cyber defenses as it main focus is on acquiring and analyzing information and not on damaging the network, it can act as a preparation phase for an attack [19]. Such activities can also be conducted out in order to disseminate information and propaganda [20]. To steal important computer data, computer-network activities can also be undertaken. Wire taps and key loggers are effective tools for cyber espionage in this situation [21]. External users can access software through trap doors at any moment without the computer user's awareness. A sniffer is a program used to steal usernames and passwords [22]. Table 1 summarizes the fundamental concepts and definitions of cyber-space.

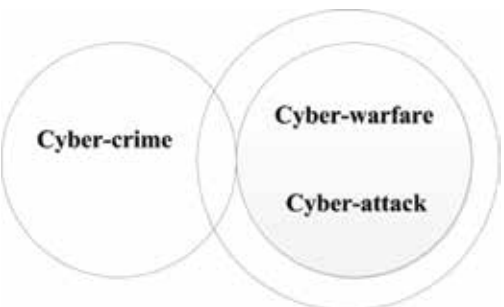
Table 1: Fundamental concepts and basic definitions of cyberspace [12] [19] [29] [30].

Concept	*Definition*
Cyberspace	Cyberspace is an interconnected network of all the communication devices worldwide including computer systems, servers, IT infrastructure, information exchange and the interaction between technology and humans for information processing, exchange, storage, retrieval and utilization.
Cyber capital	Sensitive infrastructure, critical network systems, critical information, or citizens of a country.
Cyber vulnerability	A flaw in security program, or internal control, or in the implementation of cyber asset, which may be exploited or triggered by an internal or foreign adversary to perform cyber-attack.
Cyber-threats	Any incident that has the potential to disrupt cyber space such as illegal access, disclosure, destruction or manipulation of information, and/or blockage/disruption of service delivery.
Cyber-threat-level	Cyber threat levels can be distinguished as: individual, provisional, institutional, critical infrastructure, national and international.
Cyber threats probability	Probability of cyber threats can be categorized as: imminent, probable, unlikely, very unlikely.
Cyber threats intensity	Intensity of cyber threats can be classified as disaster (very high), crisis (high), major security incident (moderate), normal security incident (low) and small security incident (very low).
Cyber attack	A cyber-attack is defined as any illegal cyber action targeted at breaking cyber asset security policies and inflicting harm, disruption, or interruption of services or access to information on cyber assets in that jurisdiction. A cyber-attack is also defined as the intentional use of cyber weapons against information systems that results in a cyber-incident.
Cyber weapon	Cyber weapons are systems that are intended and built to interfere with the structure or functioning of other cyber systems. Botnets, logic bombs, network exploits, malware, and traffic creation systems are examples of technologies used to prevent service attacks and distributed services.
Cyber-warfare	It is the highest degree and most intricate cyber-attacks carried out against various nations' cyber interests and has the most devastating implications.
Cyber warfare origin	An aggressor state or group under an aggressor state organization control or abandons cyber power and cyber weapons.
Cyber defense	Deterrence, prevention, preventive, quick detection, effective, and deterrent reaction to any cyber assault using all unarmed cyber and non-cyber facilities of a nation
Cyber-biome	The construction of native and dynamic cyber environments that assist a nation in numerous domains is referred to as a cyber-biome.
Computer Virus	A computer virus is a piece of code that replicates itself and spreads to other programs, causing the programs to malfunction. NIMDA, SLAMMER, and SASSER are several well-known viruses.
Computer Hacker	A person who gains an unauthorized access to a system or information in order to read, copy, delete, replace or destroy data.

Cyberwarfare may have the following implications [23] [5] [24]:

- Overthrow the governing system or constitute a catastrophic danger to national security;
- Begin traditional warfare at the same time to assist the start of physical combat;
- Causing catastrophic damage or harm to the country's image on a global scale;
- Causing severe disruption or harm to the country's political and economic connections;
- Internal turmoil; mass casualties or a threat to public health and safety;
- State administration is being disrupted on a large scale;
- Undermining public trust or national, religious and ethnic beliefs;
- Serious economic harm to the country;
- Widespread interruption or disruption of cyber systems.

In addition to these, five scenarios may also be considered for cyber warfare: (1) governments sponsored cyber-attacks to acquire information for future attacks, (2) cyber-attacks intended at laying the framework for any disturbance or public movement, and (3) cyber-attacks aiming at causing harm. In cyberattacks that impair equipment and aid physical assaults, (4) cyberattacks that supplement physical attacks, and (5) cyberattacks with the ultimate purpose of widespread devastation or disruption (cyber warfare) [25]. Encryption is one sort of cyber assault. Encryption is a reversible technique of encrypting data that necessitates the use of a key to decrypt. Encryption can be used in tandem with encryption to give an additional degree of secrecy [26]. Encryption is the practice and study of encrypting and decrypting data such that it can only be decoded by a certain individual. The cryptosystem is the system used to encrypt and decode data [27]. Encryption is a strong tool for securing sensitive and private information from strangers and criminals, as well as concealing unwanted behavior from law enforcement. Cryptographic techniques require continual integration to reduce vulnerabilities as computers get faster and failover solutions become more secure [28]. It is important to note that there is a distinction between cybercrime, cyberwarfare, and cyberattack in general. Figure 3 and Table 2 demonstrate the conceptual contrast between cybercrime, cyberwarfare, and cyberattack.



(Figure 3: Conceptual contrast between cybercrime, cyberwarfare, and cyberattack)

Table 2: Conceptual contrast between cybercrime, cyberwarfare, and cyberattack [31] [32].

Type	*Features*
Cyber_Crime	Actions taken in cyber space by an individual or organization usually by non-governmental attackers in violation of criminal law and is carried out through the help of computer system.
Cyber_Attack	To disrupt of destroy the working operation of a computer network.
Cyber_Warfare	The warfare conducted between nations for political or security purposes in the cyberspace and is similar or more deadly to an armed attack.

3.1 Specialists' Point of View

Experts in the legal and technological disciplines have devised a variety of definitions of cyberattack, the most notable of which are as follows:

According to Richard Clark, a cyberattack is an activity taken by a state to enter a computer or computer network in one or more nations with the intent of causing harm or destruction [33]. In the examination and critique of this definition, it can be stated that the perpetrator of the assault, the goal of the attack, and the intent of the attack are three factors as the standard, without taking into account the type of harm [34]. In addition, only the state is often recognized as the perpetrator of an assault if the attack is begun by a person in a context and geographic region (the cyberspace of a state-controlled network) under the control and jurisdiction of a state. If NGOs and private organizations conduct action against foreign nations, they are mainly beyond the scope of the preceding description and are not covered, leaving a vacuum in the legal coverage of such actions. Given this position, it is reasonable to conclude that the above definition is essentially inadequate, since it excludes the majority of assaults carried out by private and non-governmental organizations, resulting in a void [31].
Michael Hayden: Any purposeful effort to destroy or disrupt another country's computer network [35]. Obviously, this term is also quite broad and makes no distinction between cybercrime, cyberattack, and cyberwarfare, and the borders between their detection are blurred, and the lack of this distinction will undoubtedly affect critics and policymakers. The wide framework of the norms of war allows for unfettered internet, which will undoubtedly have harmful and negative repercussions for the expansion of war and the belligerence of states [36]. So, the preceding definition's generality is also its fundamental flaw, resulting in a lack of luck. In contrast to the first definition, which confined the perpetrator of an assault to a government aggressor, this term is broad, simple to interpret, and, as previously said, may be harmful, have bad consequences, and lead to international conflicts. Relations are tumultuous, and they eventually constitute a danger to international peace [37].

Martin Libicki: A digital assault on a computer system causes the targeted computer system to look normal while creating and sending out erroneous replies [38]. This definition of a cyber-assault effectively eliminates a wide variety of possible dangers to the national security of nations whose cyber infrastructure has been targeted but has not yet reached the degree and threshold of substantial attack. The fact is that these threats can inflict harm to the target country's computer systems and networks. As a result, any definition of cyber assault that excludes the aforementioned is unavoidably inadequate and not necessarily

comprehensive [39] [40].

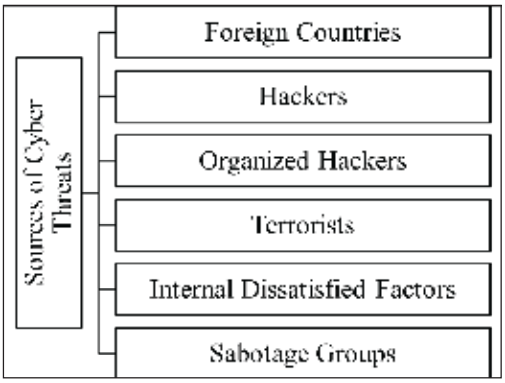
Tallinn Manual Group: A cyber-attack is a malicious or defensive cyber action that causes casualties, property damage, or destruction. The issue of contention with this definition is the produced outcome and effect. According to the source of this definition, a cyber-attack is of the attack type if it results in the outcomes indicated in the definition (i.e., causing bodily and economic harm) [29]. As a result, rather than the attack itself, the main basis for this group's definition is the result-oriented nature of a cyber-attack; such an attack can be described as an attack if it leaves an objective, tangible, violent effect and consequence, while at this stage, the rules of international law in relevant fields and areas (right to resort to duress, the law of war, and the law of international responsibility will be enforceable [41].

4. Cyberspace Threats

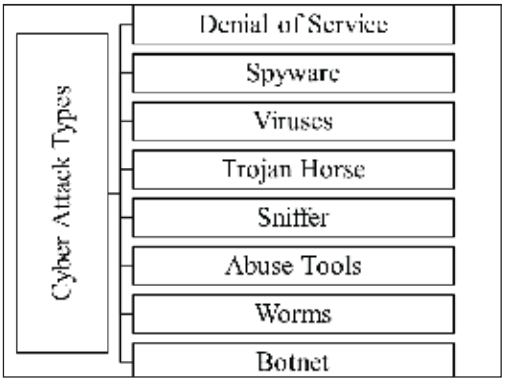
Naturally, the scale of global cyberspace produces overlapping spheres of control for state actors with varying cultural and legal approaches as well as strategic goals [42]. Countries all around the world already rely significantly for communication and control of the real world on cyber space. As a result, cyberspace is progressively influencing state security responsibilities and functions [43]. There is no certainty in the product supply chain process due to worldwide manufacture of hardware and software goods. The network realm is qualitatively distinct due to its scalability. Bombs have a limited physical reach in the most extreme situations; but, the reach of cyber threats is quite vast; hence, we have a method by which we may regulate real-world activities. Cyberspace activities, like many other disciplines of expertise, are controlled by a small number of people. Users are unable to change or control the software and hardware that they utilize. To manage and control cyber warfare there are only few organizations that are capable and it is no secret [44]. Despite the requirement for focus and competence, the scattered structure of the cyber world prohibits a single individual or group of people from gaining total control. Changes in the networking industry are occurring at a rapid pace and are based on the ongoing development of computing and communication technology. This acceleration is aided by network cohesiveness. Every transition ushers in a new period of sensitivity and responsiveness. Cyberspace, far from being stagnant throughout [45], is nearly dynamic. The distribution of cyber assets is similar to all sorts of organizations, ranging from closed and government-controlled systems to those owned and managed by society's private sector, each with various resources and facilities, as well as varied skills and concerns [46]. Because of the nature of cyberspace, there is currently no technical capability to confidently attribute actions to people, groups, or organizations. External threats, internal threats, threats in the supply chain of products and services, and risks owing to poor operational capabilities of local forces are the primary dangers in cyberspace [47]. Some intelligence collecting and espionage actions are carried out by foreign intelligence services using cyber technologies. Many similar examples have been documented throughout the world as a result of the exploitation and disruption of national information infrastructure, such as computer systems, Internet information networks, and processors

and controllers implanted in critical sectors. Another source of assaults is groups who target network systems for profit, and the number of attacks by these groups is growing [48]. In addition, other organizations (hackers) occasionally infiltrate the network to express themselves. In the current state of affairs, it is feasible to enter the network with minimum knowledge and abilities by obtaining the essential applications and protocols from the Internet and utilizing them for other sites. Simultaneously, another politically motivated organization known as hacktivism launched attacks on major online pages or email providers. These organizations often raise the burden on email providers and distribute their political messages through website infiltration [49]. Dissatisfied agents within an organization, on the other hand, are a key source of cybercrime, and these agents do not require a great deal of understanding about cyberattacks; since their target system awareness typically provides unlimited access to the system or takes the company's information. Terrorists are another source of risks because they aim to damage, disable, or deliberately exploit vital infrastructure in order to endanger national security, create large losses, harm national economies, and disrupt public attitude and confidence [50]. Figure 4 depicts the origins of cyber-attacks.

Denial of service, logic bombs, abuse tools, sniffers, Trojans, viruses, worms, spam, and botnets are the most common cyber assault tactics. Figure 5 depicts many forms of cyber-attacks. The authorized user's access to the system is denied in a denial of service attack, and vice versa. In fact, the attacker eventually immerses the target machine in numerous messages and disrupts legal data flow. This stops any system from connecting to the Internet or interacting with other systems [51]. They attack from a huge number of distributed systems at the same time in another strategy known as wide denial of service. This is commonly accomplished by spreading worms across numerous computers in order to assault the target. The public can use abusive tools to find and penetrate weaknesses in networks with differing skill levels. Another sort of attack is logic bombs, in which programmers add code into a software that automatically conducts damaging operations whenever a specified event happens [52] [53]. A sniffer is a software that listens in on routing information and searches for particular information such as passwords by inspecting each packet in the data stream [54]. Trojans conceal deadly code and frequently masquerade as beneficial applications that victims are prepared to use [55]. Viruses also taint system files, mainly utilities, by introducing copies of themselves into these files. These versions execute by loading the infected file into memory, allowing the virus to infect subsequent files. Viruses, unlike worms, require human assistance to propagate. A worm, on the other hand, is a self-replicating system software that copies itself from one computer to another on a network [56]. Finally, a botnet is a network of compromised remote control devices that are used to distribute malware, coordinate assaults, spam, and steal data. Botnets are often deployed discreetly on target computers, allowing unauthorized individuals to remotely manipulate the target system in order to achieve their harmful objectives. Botnets are frequently referred to as "electronic troops" [57].



(Figure 4: Cyber threat sources)



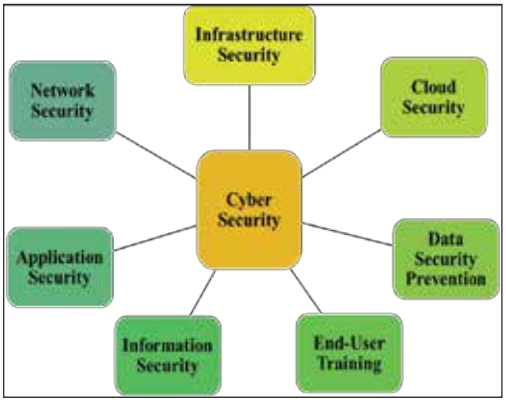
(Figure 5: Cyber-attack types.)

Qiu and his colleagues investigated the impact and danger of cybersecurity in a WAMS-based FFR (fractional flow reserve) control using a unique scale CNN to interpret faked data from two scales [58]. They are also researching a cybersecurity defensive strategy for FFR systems based on time and frequency. The results reveal that true synchro phasor data is more accurate and robust. Based on knowledge-based hidden Makrove modelling, Lee and his colleagues created a way to unify the cyberattack recovery process [59]. They also investigated a safe state approximation approach based on the updated HMM. A case study demonstrates the efficacy of the presented strategy. Zhang and Malacaria developed a cybersecurity decision support system to help organizations choose the appropriate security combination to fight against multi-stage assaults [60]. To identify ongoing threats, the system includes LM-powered online and preventative improvements. They discovered a Bayesian STACKELBERG game of selecting efficient solutions online. Kim and his colleagues investigated NPP for cyberattack likelihood factors [61]. Furthermore, AHP and FA are used to quantify the comparative importance of NPP likelihood factors. They discovered that support for South Korea's approach to cybersecurity was associated with a stronger preference for execution. According to Tosun, the cyberattack had an immediate detrimental impact on the company's reputation. Furthermore, financial markets have increased in a rebound drop in response to corporate security breaches. Furthermore, transaction rates have risen as a result of selling pressure and improved liquidity. R&D and dividends fall with time, whereas target firms continue to pay CEOs [62].

5. Mitigation Techniques – Cyber Security

Cybersecurity is a critical concern in the infrastructure of any business and organization. In brief, a cybersecurity-based firm or organization can gain high status and numerous accomplishments as a consequence of the company's capacity to secure private and consumer data from rivals. Customers' and individuals' competitors, as well as organizations, are abusive. In order to thrive and flourish, a firm or organization must first provide the highest available security [63]. Cybersecurity is taking real steps to secure information,

networks, and data from internal and external threats. Cybersecurity experts safeguard networks, servers, intranets, and computer systems. Cybersecurity guarantees that only those who are permitted have access to this information [12]. Understanding the different forms of cybersecurity is essential for effective defense. Figure 6 depicts the many forms of cybersecurity.



(Figure 6: Types of cyber security)

Network-Security: To safeguards computer networks against viruses and hackers. Cybersecurity refers to a collection of solutions that allow firms to protect computer networks against hackers, organized attacks, and viruses [64].

Application Security: The use of software like antivirus applications, encryption, and firewalls or the use of hardware devices to secure systems from threats that may interfere with application development [65].

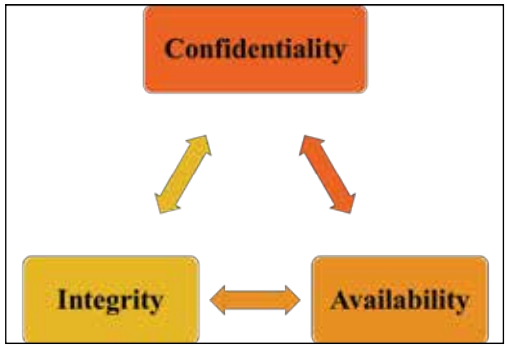
Information Security: The digital data must be protected from misuse, disclosure, unauthorized access, unlawful change, and deletion [66].

Operational security: The methods and decisions taken to regulate and secure data are referred to as operational security. For example, user privileges when connecting to a network, or processes that determine when and where information can be kept or exchanged [66].

Cloud Security: Cloud security is the process of protecting information/data stored in the cloud through tools and monitoring it in order to remove the possibility of on-site assaults [67].

User training: Individuals are the unexpected parts of cybersecurity. A virus can be inadvertently infected into a security system by anyone. Teaching employees to not to connect anonymous USB drives, to remove suspicious attachments in emails and other crucial concerns should be part of every corporate security policy [67].

Cybercrimes can be any actions that are unlawful and are performed to compromise a system, device or network. It can be categorized in two types: crimes that target systems and crimes in which systems operate inadvertently. Table 3 depicts the strategies most typically employed by cybercriminals. Any organization's security must have three principles: Confidentiality, Integrity, and Availability. These three principles are known as the CIA Triad and they have been the norm for system security from the early days of computing (see Figure 7) [68].



(Figure 7: CIA Triad)

Table 3: Strategies most typically employed by cybercriminals.

Method Name	*Description*
Denial_of_Service (DOS)	To disrupt the services of a computer system by exhausting all the network resources of the system. As a result system users can get access to it [19].
Man_in_the_Middle	To eavesdrop the communication between victim and server by sniffing the network traffic. Attacker can even change data packets [72].
Computer Malware	To infect victims using computer viruses or worms [36].
Phishing	To make user disclose his personal or organizations confidential information by using physiological techniques using emails or other platforms [50].

According to the Confidentiality concept, only those who have proper authorization can have access to sensitive information and can make use of sensitive functionalities of an organization. According to the Integrity concept, only authorized personnel are permitted to edit, remove or delete sensitive information and functions. According to the Availability concept, systems, services, and data must be made available on demand in accordance with specified specifications based on SLA service levels [69]. The greatest cybersecurity procedures go above and beyond the aforementioned criteria. This basic protection can be circumvented by any competent hacker. As a company grows in size, cybersecurity gets increasingly complex. Another cybersecurity restriction is coping with the increasing number of persons participating in the flow of virtual and real-world data. The shortage of skilled vocations to do the work is a significant barrier in cybersecurity. Many are at the bottom end of the cybersecurity vision, with general abilities. Coverage of cyberspace is a big topic. In the next essay, we'll go through the many sorts of cybersecurity. A complete approach takes into account all of these factors and does not overlook any of them [70]. The world's key infrastructure is a hybrid of cyber and physical components. This amazing building provides us with several advantages. Deploying online systems, on the other hand, introduces additional vulnerabilities for hackers and cyberattacks. Organizational decision-makers must priorities how an assault impacts their performance. Some of the most talented new hackers regard web application security as the weakest link in the chain of attack on corporations. This reduces the amount of labor required to hack and infiltrate the information. Cybersecurity is getting increasingly sophisticated. Businesses must have a "security perspective" on how cybersecurity works. Because of heightened security dangers, investments in cybersecurity systems and services are expanding. McAfee, Cisco, and Trend Micro are three businesses that are involved in this space [71].

5.1 Cyber-Security Policy

Over time, the network boosts community production and effectively distributes knowledge. No matter whatever application or industrial network is used, the goal is to increase output. The rapid movement of data to cyberspace primarily undermines the entire system's security. Security metrics are frequently in direct opposition with progress for technical experts enhancing production, since preventative measures decrease, ban, or delay user access, consume metrics that indicate impor-

tant system resources, and respond to management concerns [73]. The term "policy" refers to rules and regulations for the dissemination of information, data protection objectives for the commercial sector, and system operational policies for technological controls in a number of domains relevant to cybersecurity. However, the word cybersecurity policy is used for a distinct reason in this field. There is no definitive definition of cybersecurity policy, as there is for the word "cyberspace," but when used as an adjective in the policy area, it alludes to a common notion [74].

Cybersecurity rules are recognized by the regulatory framework and explicitly applied to the regulator's relevant areas. The components of security policies differ depending on the policy scope [75]. National cybersecurity policy, for example, applies to all citizens and maybe international businesspeople operating in the industry, but corporate cybersecurity only applies to personnel who are hired or have legal contracts and are required to manage their behavior toward the organization. It is not realistic to expect resource suppliers that are totally dependent on one client to comply with client security standards unless a written contract is in existence [76]. National security objectives are not the same as business security objectives. The implementing agency is in charge of interpreting and registering the policy, and the regulatory committee and appropriate authorities are in charge of approving it. However, in most businesses, a centralized security department is in charge of cybersecurity policies, standards, and solutions. The enterprise security unit's standards and solutions serve as a reference for legislation. When security becomes a high concern for a company, cybersecurity rules are published by various internal units of the Common Component Wing. These shared components can occasionally detect policy discrepancies caused by attempting to implement these concerns concurrently [38].

The country's cyber policy is now integrated into its national security strategy. Indeed, policies are formed and disseminated in papers and lectures via discussions and debates of many points of view. Rules and regulations have nothing to do with policies. Laws, agreements, and guidelines, at best, offer a meaningful and logical policy. Cybersecurity enforcement orders, rules, and regulations, on the other hand, can be issued without the creation of a cybersecurity policy [77].

Different sectors are required to respect the norms in a corporate environment owing to the threat of fines, which will remain until the violating sector closes. For example, code HR, civil, or costing policies such that any violation of notification rules results in the closure of the relevant department. Middle managers are required to implement communication policies into departmental operations and generate metrics at the departmental level to measure policy compliance, as well as to assist procedures such as hiring personnel or submitting costs. Any sort of organizational division has governance limits in the public sector [78]. There are instances in which different aspects of information categorization are significantly weighted, but the corporate security policy supplied by the CEO applies to the whole firm, but the security policy released by the CEO is confined to the domain. Technicians should apply. One of the most recent organizational-wide improvements has been the appointment of senior data security managers or senior

managers in charge of choosing various aspects of an organization's security posture. Also, one of the disadvantages of corporate cybersecurity policy against HR/legal policy is that it is delegated to middle management. When the danger of disclosure of sensitive information is considerable, cybersecurity regulations may demand that information not be delivered without a comprehensive review of the recipient's capacity to preserve the security of the information [79]. The policy defers data risk assessment to managers who may seek to save money by outsourcing information flow to the office and utilizing personnel outside the office for information analysis. Perhaps the same boss wishes to avoid inspection in order to reduce expenditures. This circumstance may be the consequence of a miscalculation of non-security professionals' information obligations, or it may be that the culture of the organization involved accepts the risk. In every scenario, work division is critical. These circumstances are exacerbated by the fact that cybersecurity measurements have not yet developed as accounting or HR metrics.

6. Conclusion

Cyber space and associated technologies are an important sources of power for current generation. The asymmetry of cyberspace along with anonymity and lack of security measures plus the low cost to access internet creates a situation of power dissipation. Because of which along with the measure taken at governmental level, individuals and private organizations have to also put in effort against the malicious actors in cyber space. Cyber-attacks jeopardize the national security, and its impact may be measured in various ways. The first is that the national security can no longer be defined solely in terms of internal and external boundaries; technological advancements in people's daily life pose a threat to national security as well due to interlinked services. The second is the removal of geographical boundaries of cyber threats; military threats used to have a definite geographical location with which it was easy to identify security threats but that's not the case in terms of cyber space. The third factor is the varying level of vulnerabilities brought by cyber threats; the attacks and intermittent, multi-dimensional and extremely damaging due to their link with the critical infrastructure and networks. Fourth is that the traditional tools used by security agencies for the mitigation and containment of threats are insufficient. Governments alone cannot cope with all these variables. Effective bilateral collaboration between governments and the business sector is mutually beneficial in dealing with these threats. Fifth, as seen in the preceding point, cyber risks are not restricted to governments, and people and businesses are not immune to them. In the end, only with a collective effort and use to proper tools along with adequate knowledge can the threats of cyber-attacks in cyber space be minimized.

7. References

[1] Tan, Sen, Peilin Xie, Josep M. Guerrero, Juan C. Vasquez, Yunlu Li, and Xifeng Guo. "Attack Detection Design for Dc Microgrid Using Eigenvalue Assignment Approach." *Energy Reports*, ICPE 2020-The International Conference on Power Engineering, 7 (April 1, 2021): 469–76.

[2] Judge, Malik Ali, Awais Manzoor,

Carsten Maple, Joel JPC Rodrigues, and Saif ul Islam. "Price-Based Demand Response for Household Load Management with Interval Uncertainty." *Energy Reports* 7 (2021): 8493–8504.

[3] Aghajani, Gholamreza, and Noradin Ghadimi. "Multi-Objective Energy Management in a Micro-Grid." *Energy Reports* 4 (November 1, 2018): 218–25.

[4] Akhavan-Hejazi, Hossein, and Hamed Mohsenian-Rad. "Power Systems Big Data Analytics: An Assessment of Paradigm Shift Barriers and Prospects." *Energy Reports* 4 (November 1, 2018): 91–100.

[5] Priyadarshini, Ishaani, Raghvendra Kumar, Rohit Sharma, Pradeep Kumar Singh, and Suresh Chandra Satapathy. "Identifying Cyber Insecurities in Trustworthy Space and Energy Sector for Smart Grids." *Computers & Electrical Engineering* 93 (July 1, 2021): 107204. https://doi.org/10.1016/j.compeleceng.2021.107204.

[6] Amir, Maral, and Tony Givargis. "Pareto Optimal Design Space Exploration of Cyber-Physical Systems." *Internet of Things* 12 (December 1, 2020): 100308.

[7] Li, Nianyu, Christos Tsigkanos, Zhi Jin, Zhenjiang Hu, and Carlo Ghezzi. "Early Validation of Cyber–Physical Space Systems via Multi-Concerns Integration." *Journal of Systems and Software* 170 (December 1, 2020):

[8] Niraja, K. S., and Sabbineni Srinivasa Rao. "A Hybrid Algorithm Design for near Real Time Detection Cyber Attacks from Compromised Devices to Enhance IoT Security." *Materials Today: Proceedings*, 2021.

[9] Sarker, Iqbal H. "CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks." *Internet of Things* 14 (June 1, 2021): 100393.

[10] Shin, Jinsoo, Jong-Gyun Choi, Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Jun-Young Son. "Application of STPA-SafeSec for a Cyber-Attack Impact Analysis of NPPs with a Condensate Water System Test-Bed." *Nuclear Engineering and Technology* 53, no. 10 (2021): 3319–26.

[11] Snehi, Manish, and Abhinav Bhandari. "Vulnerability Retrospection of Security Solutions for Software-Defined Cyber–Physical System against DDoS and IoT-DDoS Attacks." *Computer Science Review* 40 (May 1, 2021): 100371.

[12] Ahmed Jamal, Alshaibi, Al-Ani Mustafa Majid, Anton Konev, Tatiana Kosachenko, and Alexander Shelupanov. "A Review on Security Analysis of Cyber Physical Systems Using Machine Learning." *Materials Today: Proceedings*, July 8, 2021.

[13] Cao, Jie, Da Ding, Jinliang Liu, Engang Tian, Songlin Hu, and Xiangpeng Xie. "Hybrid-Triggered-Based Security Controller Design for Networked Control System under Multiple Cyber Attacks." *Information Sciences* 548 (February 16, 2021): 69–84.

[14] Gupta Bhol, Seema, JR Mohanty, and

Prasant Kumar Pattnaik. "Taxonomy of Cyber Security Metrics to Measure Strength of Cyber Security." *Materials Today: Proceedings*, June 24, 2021.

[15] Furnell, Steven, and Jayesh Navin Shah. "Home Working and Cyber Security – an Outbreak of Unpreparedness?" *Computer Fraud & Security* 2020, no. 8 (August 1, 2020): 6–12.

[16] Alhayani, Bilal, Sara Taher Abbas, Dawood Zahi Khutar, and Husam Jasim Mohammed. "Best Ways Computation Intelligent of Face Cyber Attacks." *Materials Today: Proceedings*, March 10, 2021.

[17] "Riskio: A Serious Game for Cyber Security Awareness and Education - ScienceDirect." Accessed March 27, 2022.

[18] Ma, Lei, Ying Zhang, Chunyu Yang, and Linna Zhou. "Security Control for Two-Time-Scale Cyber Physical Systems with Multiple Transmission Channels under DoS Attacks: The Input-to-State Stability." *Journal of the Franklin Institute* 358, no. 12 (August 1, 2021): 6309–25.

[19] Alghamdie, Mohammed. I. "A Novel Study of Preventing the Cyber Security Threats." *Materials Today: Proceedings*, April 23, 2021. https://doi.org/10.1016/-j.matpr.2021.04.078.

[20] Thomson, J. R. "Chapter 3 - Cyber Security, Cyber-Attack and Cyber-Espionage." In *High Integrity Systems and Safety Management in Hazardous Industries*, edited by J. R. Thomson, 45–53. Boston: Butterworth-Heinemann, 2015.

[21] Liu, Xiaoxue, Jiexin Zhang, Peidong Zhu, Qingping Tan, and Wei Yin. "Quantitative Cyber-Physical Security Analysis Methodology for Industrial Control Systems Based on Incomplete Information Bayesian Game." *Computers & Security* 102 (March 1, 2021): 102138.

[22] Karbasi, Ali, and Alireza Farhadi. "A Cyber-Physical System for Building Automation and Control Based on a Distributed MPC with an Efficient Method for Communication." *European Journal of Control* 61 (September 1, 2021): 151–70.

[23] Khan, Shah Khalid, Nirajan Shiwakoti, Peter Stasinopoulos, and Yilun Chen. "Cyber-Attacks in the next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions." *Accident Analysis & Prevention* 148 (December 1, 2020): 105837.

[24] Mehrpooya, Mehdi, Noradin Ghadimi, Mohammad Marefati, and Sohrab Ali Ghorbanian. "Numerical Investigation of a New Combined Energy System Includes Parabolic Dish Solar Collector, Stirling Engine and Thermoelectric Device." *International Journal of Energy Research* 45, no. 11 (2021): 16436–55.

[25] Alibasic, Armin, Reem Al Junaibi, Zeyar Aung, Wei Lee Woon, and Mohammad Atif Omar. "Cybersecurity for Smart Cities: A Brief Review." In *Data Analytics for Renewable Energy Integration*, edited by Wei Lee Woon, Zeyar Aung, Oliver Kramer, and Stuart Madnick,

22–30. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-50947-1_3.

[26] Sun, Chih-Che, Adam Hahn, and Chen-Ching Liu. "Cyber Security of a Power Grid: State-of-the-Art." *International Journal of Electrical Power & Energy Systems* 99 (July 1, 2018): 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020.

[27] ji, Zuzhen, Shuang-Hua Yang, Yi Cao, Yuchen Wang, Chenchen Zhou, Liang Yue, and Yinqiao Zhang. "Harmonizing Safety and Security Risk Analysis and Prevention in Cyber-Physical Systems." *Process Safety and Environmental Protection* 148 (April 1, 2021): 1279–91. https://doi.org/10.1016/j.psep.2021.03.004.

[28] Zou, Tierui, Arturo S. Bretas, Cody Ruben, Surya C. Dhulipala, and Newton Bretas. "Smart Grids Cyber-Physical Security: Parameter Correction Model against Unbalanced False Data Injection Attacks." *Electric Power Systems Research* 187 (October 1, 2020): 106490. https://doi.org/10.1016/j.epsr.2020.106490.

[29] Bullock, Jane A., George D. Haddow, and Damon P. Coppola. "Chapter 8 - Cybersecurity and Critical Infrastructure Protection." In *Introduction to Homeland Security (Sixth Edition)*, edited by Jane A. Bullock, George D. Haddow, and Damon P. Coppola, 425–97. Butterworth-Heinemann, 2021.

[30] Ashraf, Javed, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D. Bakhshi, and Reham R. Mostafa. "IoTBoT-IDS: A Novel Statistical Learning-Enabled Botnet Detection Framework for Protecting Networks of Smart Cities." *Sustainable Cities and Society* 72 (September 1, 2021): 103041.

[31] Zhang, Ting. "A Comparative Study on Sanction System of Cyber Aider from Perspectives of German and Chinese Criminal Law." *Computer Law & Security Review* 33, no. 1 (February 1, 2017): 98–102.

[32] Dash, Nitu, S. Chakravarty, and Suneeta Satpathy. "An Improved Harmony Search Based Extreme Learning Machine for Intrusion Detection System." *Materials Today: Proceedings*, February 26, 2021.

[33] Motsch, William, Alexander David, Keran Sivalingam, Achim Wagner, and Martin Ruskowski. "Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems." *Procedia Manufacturing*, 30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2021), 51 (January 1, 2020): 1748–54.

[34] Cao, Yan, Zhiqiu Huang, Changbo Ke, Jian Xie, and Jinyong Wang. "A Topology-Aware Access Control Model for Collaborative Cyber-Physical Spaces: Specification and Verification." *Computers & Security* 87 (November 1, 2019): 101478.

[35] Robinson, Michael, Kevin Jones, and

Helge Janicke. "Cyber Warfare: Issues and Challenges." *Computers & Security* 49 (March 1, 2015): 70–94.

[36] Edgar, Thomas W., and David O. Manz. "Chapter 2 - Science and Cyber Security." In *Research Methods for Cyber Security*, edited by Thomas W. Edgar and David O. Manz, 33–62. Syngress, 2017.

[37] Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. "SCADA Security in the Light of Cyber-Warfare." *Computers & Security* 31, no. 4 (June 1, 2012): 418–36.

[38] Quigley, Kevin, Calvin Burns, and Kristen Stallard. "'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection." *Government Information Quarterly* 32, no. 2 (April 1, 2015): 108–17.

[39] Damon, Evan, Jens Mache, Richard Weiss, Kaleb Ganz, Claire Humbeutel, and Miles Crabill. "Chapter 31 - Cyber Security Education: The Merits of Firewall Exercises." In *Emerging Trends in ICT Security*, edited by Babak Akhgar and Hamid R. Arabnia, 507–16. Boston: Morgan Kaufmann, 2014.0031-1.

[40] "Designing a PID Controller to Control a Fuel Cell Voltage Using the Imperialist Competitive Algorithm - Advances in Science and Technology. Research Journal - Tom Vol. 10, Nr 30 (2016) - BazTech - Yadda." Accessed March 27, 2022.

[41] Chen, Ji-Kang, Ching-Wen Chang, Zhiyou Wang, Li-Chih Wang, and Hsi-Sheng Wei. "Cyber Deviance among Adolescents in Taiwan: Prevalence and Correlates." *Children and Youth Services Review* 126 (July 1, 2021): 106042.

[42] Iqbal, Zafar, and Zahid Anwar. "SCERM—A Novel Framework for Automated Management of Cyber Threat Response Activities." *Future Generation Computer Systems* 108 (July 1, 2020): 687–708.

[43] Zhao, Jun, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. "TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data." *Computers & Security* 95 (August 1, 2020): 101867.

[44] Zhang, Xiaoyu, Maochao Xu, Gaofeng Da, and Peng Zhao. "Ensuring Confidentiality and Availability of Sensitive Data over a Network System under Cyber Threats." *Reliability Engineering & System Safety* 214 (October 1, 2021): 107697.

[45] Varga, Stefan, Joel Brynielsson, and Ulrik Franke. "Cyber-Threat Perception and Risk Management in the Swedish Financial Sector." *Computers & Security* 105 (June 1, 2021): 102239.

[46] "Control-Theory Based Security Control of Cyber-Physical Power System under Multiple Cyber-Attacks within Unified Model Framework - ScienceDirect." Accessed March 27, 2022.

[47] Al-Ghamdi, Mohammed I. "Effects of

Knowledge of Cyber Security on Prevention of Attacks." *Materials Today: Proceedings*, April 27, 2021.

[48] Beechey, Matthew, Konstantinos G. Kyriakopoulos, and Sangarapillai Lambotharan. "Evidential Classification and Feature Selection for Cyber-Threat Hunting." *Knowledge-Based Systems* 226 (August 17, 2021): 107120.

[49] Solomon, Rukundo. "Electronic Protests: Hacktivism as a Form of Protest in Uganda." *Computer Law & Security Review* 33, no. 5 (October 1, 2017): 718–28.

[50] Saxena, Rashi, and E. Gayathri. "Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution." *Materials Today: Proceedings*, CMAE'21, 51 (January 1, 2022): 682–89.

[51] Topping, Colin, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid. "Beware Suppliers Bearing Gifts!: Analysing Coverage of Supply Chain Cyber Security in Critical National Infrastructure Sectorial and Cross-Sectorial Frameworks." *Computers & Security* 108 (September 1, 2021): 102324.

[52] Li, Jian, Chaowei Sun, and Qingyu Su. "Analysis of Cascading Failures of Power Cyber-Physical Systems Considering False Data Injection Attacks." *Global Energy Interconnection* 4, no. 2 (April 1, 2021): 204–13.

[53] Marefati, Mohammad, Mehdi Mehrpooya, and Mohammad Behshad Shafii. "Optical and Thermal Analysis of a Parabolic Trough Solar Collector for Production of Thermal Energy in Different Climates in Iran with Comparison between the Conventional Nanofluids." *Journal of Cleaner Production* 175 (February 20, 2018): 294–313.

[54] Patel, Deven C., Mark F. Berry, Prasha Bhandari, Leah M. Backhus, Shehzaib Raees, Winston Trope, Abraham Nash, Natalie S. Lui, Douglas Z. Liou, and Joseph B. Shrager. "Paradoxical Motion on Sniff Test Predicts Greater Improvement Following Diaphragm Plication." *The Annals of Thoracic Surgery* 111, no. 6 (June 1, 2021): 1820–26.

[55] Al Shaer, Danah, Othman Al Musaimi, Beatriz G. de la Torre, and Fernando Albericio. "Hydroxamate Siderophores: Natural Occurrence, Chemical Synthesis, Iron Binding Affinity and Use as Trojan Horses against Pathogens." *European Journal of Medicinal Chemistry* 208 (December 15, 2020): 112791.

[56] Aziz, Amal A., and Zareen Amtul. "Developing Trojan Horses to Induce, Diagnose and Suppress Alzheimer's Pathology." *Pharmacological Research* 149 (November 1, 2019): 104471.

[57] Kharlamova, Nina, Seyedmostafa Hashemi, and Chresten Træholt. "Data-Driven Approaches for Cyber Defense of Battery Energy Storage Systems." *Energy and AI* 5 (September 1, 2021): 100095.

[58] Qiu, Wei, Kaiqi Sun, Wenxuan Yao, Shutang You, He Yin, Xiaoyang Ma, and Yilu Liu. "Time-Frequency Based Cyber

Security Defense of Wide-Area Control System for Fast Frequency Reserve." *International Journal of Electrical Power & Energy Systems* 132 (November 1, 2021): 107151.

[59] Lee, Chanyoung, Young Ho Chae, and Poong Hyun Seong. "Development of a Method for Estimating Security State: Supporting Integrated Response to Cyber-Attacks in NPPs." *Annals of Nuclear Energy* 158 (August 1, 2021): 108287.

[60] "Bayesian Stackelberg Games for Cyber-Security Decision Support - ScienceDirect." Accessed March 27, 2022.

[61] Kim, Yong Sik, Moon Kyoung Choi, Sang Min Han, Chanyoung Lee, and Poong Hyun Seong. "Development of a Method for Quantifying Relative Importance of NPP Cyber Attack Probability Variables Based on Factor Analysis and AHP." *Annals of Nuclear Energy* 149 (December 15, 2020): 107790.

[62] Tosun, Onur Kemal. "Cyber-Attacks and Stock Market Activity." *International Review of Financial Analysis* 76 (July 1, 2021): 101795.

[63] Rodríguez-deArriba, María-Luisa, AnnaLaura Nocentini, Ersilia Menesini, and Virginia Sánchez-Jiménez. "Dimensions and Measures of Cyber Dating Violence in Adolescents: A Systematic Review." *Aggression and Violent Behavior* 58 (May 1, 2021): 101613.

[64] Zhang, Jie. "Distributed Network Security Framework of Energy Internet Based on Internet of Things." *Sustainable Energy Technologies and Assessments* 44 (April 1, 2021): 101051.

[65] Alkatheiri, Mohammed Saeed, Sajjad Hussain Chauhdary, and Mohammed A. Alqarni. "Seamless Security Apprise Method for Improving the Reliability of Sustainable Energy-Based Smart Home Applications." *Sustainable Energy Technologies and Assessments* 45 (June 1, 2021): 101219.

[66] Ogbanufe, Obi. "Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity." *Computers & Security* 108 (September 1, 2021): 102340.

[67] Krishnasamy, Vidhyanandhini, and Saravanarajan Venkatachalam. "An Efficient Data Flow Material Model Based Cloud Authentication Data Security and Reduce a Cloud Storage Cost Using Index-Level Boundary Pattern Convergent Encryption Algorithm." *Materials Today: Proceedings*, May 26, 2021.

[68] Palmieri, Michael, Neil Shortland, and Presley McGarry. "Personality and Online Deviance: The Role of Reinforcement Sensitivity Theory in Cybercrime." *Computers in Human Behavior* 120 (July 1, 2021): 106745.

[69] Nguyen, Dr. Chat Le, and Dr. Wilfred Golman. "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action.'" *Computer Law & Security Review* 40 (April 1,

2021): 105521.

[70] Alzubaidi, Abdulaziz. "Cybercrime Awareness among Saudi Nationals: Dataset." *Data in Brief* 36 (June 1, 2021): 106965.

[71] Chandra, Akhilesh, and Melissa J. Snowe. "A Taxonomy of Cybercrime: Theory and Design." *International Journal of Accounting Information Systems*, 2019 UW CISA Symposium, 38 (September 1, 2020): 100467.

[72] Huang, Jiahao, Daniel W. C. Ho, Fangfei Li, Wen Yang, and Yang Tang. "Secure Remote State Estimation against Linear Man-in-the-Middle Attacks Using Watermarking." *Automatica* 121 (November 1, 2020): 109182.

[73] Katrakazas, Christos, Athanasios Theofilatos, George Papastefanatos, Jérôme Härri, and Constantinos Antoniou. "Chapter Three - Cyber Security and Its Impact on CAV Safety: Overview, Policy Needs and Challenges." In *Advances in Transport Policy and Planning*, edited by Dimitris Milakis, Nikolas Thomopoulos, and Bert van Wee, 5:73–94. Policy Implications of Autonomous Vehicles. Academic Press, 2020.

[74] Tam, Tracy, Asha Rao, and Joanne Hall. "The Good, the Bad and the Missing: A Narrative Review of Cyber-Security Implications for Australian Small Businesses." *Computers & Security* 109 (October 1, 2021): 102385.

[75] Cheng, Shen, Gaiju Zhao, Ming Gao, Yuetao Shi, Mingming Huang, and Mohammad Marefati. "A New Hybrid Solar Photovoltaic/ Phosphoric Acid Fuel Cell and Energy Storage System; Energy and Exergy Performance." *International Journal of Hydrogen Energy* 46, no. 11 (February 11, 2021): 8048–66.

[76] Alghamdi, Mohammed I. "Determining the Impact of Cyber Security Awareness on Employee Behaviour: A Case of Saudi Arabia." *Materials Today: Proceedings*, April 29, 2021.

[77] Sakhnini, Jacob, Hadis Karimipour, Ali Dehghantanha, and Reza M. Parizi. "Physical Layer Attack Identification and Localization in Cyber–Physical Grid: An Ensemble Deep Learning Based Approach." *Physical Communication* 47 (August 1, 2021): 101394.

[78] Baig, Zubair A., Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, et al. "Future Challenges for Smart Cities: Cyber-Security and Digital Forensics." *Digital Investigation* 22 (September 1, 2017): 3–13.

[79] Arend, Isabel, Asaf Shabtai, Tali Idan, Ruty Keinan, and Yoella Bereby-Meyer. "Passive- and Not Active-Risk Tendencies Predict Cyber Security Behavior." *Computers & Security* 97 (October 1, 2020): 101964.