Journal of Software Engineering and Applications, 2023, 16, 548-560
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Cybersecurity and Domestic Terrorism: Purpose and Future

Robb Shawe, Ian R. McAndrew

The Department of Cyber Leadership, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu, irmcandrew@captechu.edu

How to cite this paper: Shawe, R. and McAndrew, I.R. (2023) Cybersecurity and Domestic Terrorism: Purpose and Future. *Journal of Software Engineering and Applications*, **16**, 548-560.
https://doi.org/10.4236/jsea.2023.1610028

Received: August 31, 2023
Accepted: October 28, 2023
Published: October 31, 2023

Abstract

The increasing utilization of digital technologies presents risks to critical systems due to exploitation by terrorists. Cybersecurity entails proactive and reactive measures designed to protect software and electronic devices from any threats. However, the rising cases of cyber threats are carried out by domestic terrorists who share particular ideologies or grievances. This paper analyzes the increasing cyber-attack instances and mechanisms to counter these threats. Additionally, it addresses the growing concern of domestic terrorism and its impact on national security. Finally, it provides an overview of gaps and possible areas of future research to promote cybersecurity.

Keywords

Cyber-Attacks, Cybercrime, Cybersecurity, Cyber Threats, Domestic Terrorism

1. Introduction

Cybersecurity is a combination of practices, processes, and technologies to protect data, mobile devices, computers, servers, electronic systems, and networks from malicious attacks [1]. Cybersecurity measures are designed to protect machines and software from cyber threats (see **Appendix A**). The world is changing based on constant technological improvements and their application to solving real-life challenges. However, terrorists are also evolving at a fast rate. Domestic terrorism is the criminal and violent acts spearheaded by individuals or groups to further their ideological agendas arising from domestic influences that include political, social, religious, environmental, or racial nature. The perpetrators of domestic terrorism carried out violent acts against their fellow citizens. The rising dependence on technology and the use of the Internet in various industries increase the vulnerability of these organizations to cybercrime and the increas-

ing threat of cyber-terrorism [2]. Hence, there is a need to address the growing incidences of cyber-attacks by domestic extremist groups to ensure the authenticity and integrity of digital information.

1.1. Statement of Problem

The resilience paper examines the relationship between increased internet connectivity and rising cyber-attack cases. Terrorism constantly changes and is viewed differently by individuals in political and social environments. There is no single way of defining terrorism. The world continues to evolve rapidly based on the advancement in technology. New technologies facilitate the continuous development of new devices, such as mobile phones and software systems [2]. Unfortunately, terrorists also adapt to technological improvements by using the Internet to recruit members into their organizations. Technology often acts as a recruitment tool or a weapon that can be employed to launch an attack on a particular system. Most industries in an economy have increased dependence on technology, making them more vulnerable to cyber-terrorism.

Moreover, cyber-attacks often damage critical infrastructures, such as causing a meltdown in nuclear power plants or hacking into the electrical system or hospital system, which can cause a malfunction of essential equipment [1]. Domestic terrorist often possesses a variety of motives behind any attack carried out. Additionally, the rationale behind any attack on cyberspace differentiates cyber-terrorism from cyber-attacks and cyber-crime. Cybercrime or cyber-attacks involve accessing a system to steal sensitive information or money or merely deleting or altering specific data. Cyber-terrorism includes a remote attack using computers or a physical attack on a computer-controlled system.

1.2. Purpose of Research

This research study aims to discuss the rising need for internet connectivity and its possible exploitation of digital technologies by cyber-attacks. In short, the analysis helps enhance cybersecurity measures. Cybersecurity involves enforcing reactive and proactive measures to ensure the authenticity, confidentiality, integrity, availability, and nonrepudiation of data found in an electronic format [3]. Cybersecurity protects cyberspace services that safeguard the sets of data stored therein. The majority of the critical infrastructure services have been digitized. Therefore, the information could contain details of private or public resources. As a result, the increasing cybercrimes by local extremist groups could disrupt operations in these systems or result in economic losses incurred while repairing the affected systems.

1.3. Research Question

What is the impact of centralized data storage on cybersecurity?

1.4. Subsidiary Questions

1) What are the factors contributing to cyber-attacks on critical infrastructure?

2) What are the measures used to protect digital information from cyber-attacks?

3) What are the methods of managing cyber-attacks?

1.5. Significance of Study

This study may be critical in understanding how increased internet connectivity impacts the integrity and authenticity of digital data. The study is also relevant as it helps identify practical measures to improve cybersecurity, ensuring the protection of digital technologies. Furthermore, it identifies possible concerns to address in society to reduce the influence of domestic extremist groups and provide mechanisms for surveillance and control through federal laws.

1.6. Delimitations of Study

The research involved a review of scholarly articles on the current state of cybersecurity and domestic terrorism in the USA. Therefore, the study did not include literature analysis from other regions, whereby the USA faces the greatest cyber-attacks by domestic extremists and international terrorist organizations.

1.7. Outline of Study

The paper summarized and critically evaluated scholarly work on cybersecurity and domestic terrorism. The review also focuses on methods, risks, and cyber-attack management to ensure cybersecurity. For this reason, it will also analyze the strengths and weaknesses of the available literature to identify gaps and areas of future work on cybersecurity.

2. Literature Review

The utilization of the Internet is rising due to the increasing need for digital connection of records and information for several industries, which include health and emergency systems, power utilities, traffic systems, and water treatment services [2]. As a result, over thirty billion devices and procedures are projected to be connected to the Internet by 2030, increasing the number of cyber-terrorists' potential targets [2].

Several reasons contribute to the increasing exploitation of cyberspace by terrorists. First, cyber-attacks are challenging to trace and identify, even with technological advancements. Terrorists can launch a cyber-attack with minimal risk of being detected or identified. Secondly, terrorists utilize a short period to exploit the vulnerability once discovered [4]. Contrastingly, institutions vulnerable to cyber-attacks take considerable time to identify and fix the issues. Thirdly, cyber-attacks can be used to remotely launch attacks on a target, saving the terrorist organizations time and money while carrying out an attack. Lastly, cyber-terrorists continue to exploit cyberspace since it is inexpensive and can be utilized several times. Unlike weapons that can only be used once, cyber-terrorism requires access and constant updates of technology that can be used to penetrate other

systems.

2.1. Methods of Cyber-Attacks

Cyber-terrorists use various methods to attack (see **Appendix B**). The techniques used include phishing, ransomware, watering hole attacks, a man in the middle, distributed denial of service, and supply chain [4]. The motives behind these attacks vary from deleting or destroying data and stealing sensitive information to gaining control of a system or defacing a website. The first mechanism that criminals use to launch a cyber-attack is phishing. Phishing entails unauthorized access to sensitive information such as passwords, usernames, credit card information, and personally identifiable information. Phishing attacks can be random, or they can target a specific person. In this manner, the episodes are carried out by sending malicious emails to potential targets that can infect their systems with viruses or facilitate easy access to their personal information.

The second method is ransomware attacks. Ransomware is a form of malware used to infect networks and systems and prevent access to the affected systems and networks until the demanded ransom is paid (see **Appendix B**). Private industries and government agencies have been targets of ransomware attacks. For instance, Baltimore, Maryland, was hit by a ransomware attack in 2019, which affected the execution of essential services in the town. The cost of the spell and recovery was estimated at over $18.6 million [4].

The third method is watering hole attacks that compromise a system the intended victim frequently uses. The attackers can plant malware into an advertisement or a banner that would then be displayed on the website. The malware spreads throughout their system once the user clicks on the infected ad.

The fourth mechanism of cyber-attacks is a man in the middle. The attacks occur when a third party intercepts information shared between entities [5]. The perpetrators of these attacks could then steal or alter the data before it is transmitted to the other entity. Finally, man, in the middle, can affect corporates where the attackers access the info and reach out to clients by impersonating the affecting entity. Again, the attacks result in enormous losses.

The fifth means of cyber-attack is distributed denial of service (DDoS). DDoS is conducted by introducing malware into networks that turn the affected systems into a botnet (see **Appendix B**). A botnet refers to a network of computers controlled as a group. The botnets direct traffic to a particular website that can overwhelm a system, causing regular traffic into the system to get a denial of access error. Such an error prevents users from accessing the affected website. For example, Twitter, Amazon, and Netflix were the targets of distributed denial of services attacks in 2016. The attacks prevented access to the websites for a day.

The last method of conducting a cyber-attack is through a supply chain attack (see **Appendix B**). Supply chain attacks occur when a software code is compromised such that attackers can gain access to a system through an insider threat, an outside partner, or a previous attack on the system. A supply chain attack im-

plies that a third party gives the attackers the software code to launch an attack.

Cyber-attacks produce the most devastating effects on a nation's critical infrastructure (see **Appendix B**). According to the World Economic Forum's Global Risk Report published in 2019, cyber-attacks are in the top ten most impactful risks. Additionally, organizations that support critical national infrastructures such as health, power, manufacturing, industry, and infrastructure experienced at least one cyber-attack between 2017 and 2019 [5]. The attacks disrupted services or data breaches. Other studies indicate that cyber-attacks are a growing threat to the information infrastructure as their impact increases.

2.2. Managing Cyber-Attacks

The Cybersecurity Operations Centre (CSOC) offers an effective defense mechanism against cyber threats. Private corporations often contract CSOC to assess and provide security measures to help provide security to their digital technologies [6]. CSOC employs several mechanisms to manage cyber-attacks. First, using sensors, CSOC monitors clients' networks for traffic and potential security concerns. The sensors have a readable intrusion detection system (IDS) that alerts unauthorized parties to access the customers' electronic data. Once these alerts are received, independent analysts are contracted to carefully analyze the signals to determine the possibility of a threat to the system.

Various strategies are used to queue alerts from the sensors for effective investigation and review of the security alerts. The first strategy is the first in, first out mechanism, where the first alert received is relayed to CSOC for evaluation regardless of the priority of the attention. The second strategy is round-robin [6]. The design allows the system to select alerts circularly received from various systems. Signals are transmitted regardless of their priority. The final strategy is called the triaging method.

In most cases, CSOC triages alerts into low priority, medium priority, and high priority. Once a workload has been created under this strategy, all the high-priority signals will be aggregated at the system's top, followed by medium-priority and low-priority alerts. The execution and evaluation of the signs follow the first-in, first-out rule.

Utilizing intrusion detection systems (IDS) within digital technologies is necessary since it facilitates the early detection of cyber threats and the subsequent implementation of strategies to counter them [6]. IDS employ pattern-matching tools to recognize an activity matching a predetermined feature set. The majority of the literature on cybersecurity has focused on developing automated systems that can detect suspicious activity on digital infrastructure. Additionally, several measures are employed to ensure the timely detection of security concerns and evaluation to reduce the impact of the attacks.

2.3. Evaluating the Risks of Cyber-Terrorism

Cyber-terrorism entails the utilization of computing tools and technologies to intimate, coerce, or shut down critical infrastructure, such as energy and trans-

portation systems, that can affect government or civilian operations [7]. Several economic sectors' increasing dependence on digital technologies increases the risk of cyber-attacks. Often, disruption of critical infrastructure is believed to cause a threat to national security. [7] argued that cyber-attacks may have minimal influence on national security depending on the definition of national security and the thresholds to determine acceptable damage. Any disruption against critical infrastructure is unacceptable from the public or legal perspective. However, from a strategic military view, an attack that does not cause significant damage to the infrastructure has minimal effect on national security. For this reason, it is necessary to differentiate terrorist acts from expected disruptions. Cyber terrorists would need to launch multiple attacks on a system and cause trouble to gain their strategic agendas for an extended period.

Terrorists' activities often cause damage and instill fear and terror in the affected victims. Even though the constant attacks on critical infrastructure such as water systems and the power grid do not produce devastating effects, they are meant to gain attention and spread propaganda. Evaluating the risks of cyber-terrorism is complicated by the tendency to attribute cyber-attacks to terrorist or military efforts, while local recreational hackers spearhead most of these attacks [7]. Moreover, overdependence on an internet-accessible network increases the risk of espionage. Espionage has a greater risk compared to a cyber-attack on national security. In some instances, espionage activities are conducted by terrorist groups, where they exploit internet vulnerabilities to gain access to the targeted systems. The perpetrators of the crimes can also access a plan to gather intelligence, especially on publicly available matters. Aside from hacking, potential terrorists can create a backdoor to access the targeted system without causing any disruption. Such access focuses on gathering intelligence that can be used to carry out future attacks.

A critical review of cyber-attacks prevents two crucial lessons. First, digital infrastructures are flexible and agile but brittle, making them porous. The brittle nature of digital systems affects the defense of the systems, explaining the continued growth of the attacks and the escalation of their effects [7]. The widespread availability and use of digital technologies create a wider surface for cyber-attacks to occur and increase the number of successful attacks. Secondly, the reviews indicate inadequate mechanisms framed to govern cybersecurity. Despite the growing efforts of state actors and private institutions to develop measures to improve the security of infrastructures and information systems, the number and impact of cyber-attacks continue to rise. Furthermore, the inadequacy of cybersecurity measures can negatively affect the development of information societies worldwide.

An efficient information revolution around the globe can occur in international stability and trust. Cyber threats undermine the constancy of information societies. Digital technologies are a source of development as well as risks. However, the occurrence of cyber-attacks can contribute to instability in a country.

For instance, the cyber-attacks that the USA and Russia supposedly launched against each other in 2018 and 2019 indicate how cyber threats primarily affect national and international stability. In addition to its effects on strength, cyber-attacks negatively affect public trust [7]. The rising number of attacks on personal networks and systems could erode users' trust, preventing innovation and the adoption of digital technologies.

3. Treating Cybersecurity as a Public Good

Reconsidering the frameworks to secure digital technologies relies on cybersecurity governance. Cybersecurity should be treated as a public good managed in the public interest [8]. Cyber contains a wide range of information on the physical, social, political, and economic elements, making its security essential as it promotes technological progress and societal development and harnesses the capability of social technologies to deliver socially acceptable outcomes. Cybersecurity includes various practices such as software and network security, architecture, surveillance, risk assessment, cryptography, disaster management, and physical essentials. When considering cybersecurity governance, a distinction between scopes, actors, and cybersecurity practices must be made.

Cybersecurity has three domains at the highest abstracted level. First, it should have a robust engineering system, indicating it can withstand attacks. Secondly, the system should contain mechanisms designed to detect any anomaly or threat, guaranteeing resilience. Lastly, a system's stability determines its responses to attacks.

Ideally, the system's robustness, strength, and reactions toward an attack should qualify as a public good. However, [6] argued that the robustness of a cybersecurity system allows for the public interest, while that is different for the response and resilience of the system. Simultaneously, robustness facilitates the design of a reliable and solid technique, stability, and response work to reinforce its capabilities. Moreover, this explains why robustness should be treated as a public good rather than response or resilience. Additionally, the high cost of a systems' response and resilience mechanisms can affect the public interest and mislead cybersecurity governance.

A system's robustness defines a system's divergence between actual and expected behavior when fed with erroneous inputs. The size of the separation between the virtual and anticipated conduct determines whether such a system is more or less robust [8]. Even though the robustness of a system is not sufficient, it is necessary to ensure reliable systems by mitigating them against the effects of attacks. Similarly, enhancing the robustness of a system is costly as it requires the development of an accurate design, validation and verification of code, and probing and testing for vulnerabilities. Thus, designing a robust cybersecurity system is not exhausted by its use (that means it is club good), but its uptake is regulated by its cost.

Considering the current escalation of cyber threats, the club's good nature of

cybersecurity robustness has yet to be practical. Market collaboration is needed to ensure an even distribution that can withstand attacks. Robustness should be built into the digital endpoint of devices to offset its cost. Developing a robust system has direct and indirect implications for utilizing information societies. For instance, it can enable public infrastructures to work smoothly and allow internet users to conduct their activities successfully while relying on a secure system. Therefore, robustness can be treated as a public good once its cost has been managed to ensure free access. Robustness should be availed in all digital technologies to ensure users have access to systems whose robust nature meets the context and purpose of deployment.

Managing cybersecurity as a public good is advantageous. First, it presents a systemic approach to the security of digital technologies. Addressing a public interest requires evaluating indirect and direct externalities and medium and long-term effects. The systemic approach focuses on the interdependence of different yet interconnected technologies and their impact based on their deployment and the public interest at stake. Secondly, it promoted shared responsibility. A public good is often managed through public and private sector collaboration. The public sector formulates standards, testing and oversight procedures, and certification to maintain adequate security to foster and protect public interests. Sufficient protection also offers compensation and redressing measures to manage the system when responsibilities are not appropriately discharged.

Similarly, the private sector is tasked with designing and promoting the robustness of the products and services. The private industry also partners with the public sector for testing and controlling mechanisms. In short, the distribution of responsibilities and the need to address direct and indirect externalities promotes collaboration and information sharing regarding cybersecurity. For instance, sharing information concerning vulnerabilities in systems in a supply chain is essential as it enables the private sector to learn from its peers and design a robust system.

Significance of Cybersecurity

Cybersecurity involves enforcing reactive and proactive measures to ensure the authenticity, confidentiality, integrity, availability, and nonrepudiation of data found in an electronic format [3]. The information could contain details of private or public resources. Cybersecurity protects cyberspace services that safeguard the sets of data stored therein. The reactive and proactive measures to ensure normality include policies, standards, concepts, guides for risk management, security, training and awareness, and technical solutions designed to protect the cyberinfrastructure. Cybersecurity is considered beneficial based on its varied significance.

First, the cybersecurity organizational and conceptual frameworks promote and enhance the security culture in cyber. Secondly, it facilitates the development of international cooperation on cybersecurity concerns where the involved

parties can share information that aids in improving a system based on previous challenges or designing a robust cybersecurity system. Thirdly, cybersecurity also facilitates the development of resilient cyber infrastructure, which increases the capability to respond to cyber-crime incidents and reduce their effect on resources and services involving cyber infrastructure.

Fourthly, the proactive and reactive measures of cybersecurity work to protect data shared through cyberinfrastructure. Cybercrime perpetrators often conduct cyber-attacks that disrupt services or gain access to specific data. The increasing reliance on digital technologies further compounds security concerns. However, necessary mechanisms have been adopted to secure electronic information, ensuring its authenticity and integrity. Fifthly, cybersecurity helps cultivate the trust required for developing business and societal information in cyberspace [3]. The robustness of the cybersecurity system ensures it can withstand any cyber-attack. Therefore, internet users will likely trust the system to promote continued use. It also boosts invention and innovation in the storage and utilization of electronic data.

Lastly, cybersecurity provides avenues to exploit through democratic and participative approaches to ensure efficient cyberspace governance. As noted in the paper, the escalation of cyber-attacks is attributed to the inadequacy of the measures adopted to counteract cyber-primary. The primary mechanism proposed to improve cybersecurity governance is to treat it as a public good with shared participation, response, and possibilities. Collaboration can help design a robust system to withstand attacks, promoting information securely stored in cyberinfrastructure.

4. The Interrelationship between Cyber-Attacks, Cybersecurity, and National Security

The evolution of cyber threats in the recent past presents a set of dynamic threats to a nation's national security and economic progress. Adopting the necessary measures to prevent cybercrimes is critical to attaining cybersecurity. Each jurisdiction has designed laws to address cyber-attacks [9]. For instance, federal laws in the USA stipulate violent acts that can be attributed as an act of terrorism or not. A demonstration in Charlottesville, Virginia, in August 2017, led by white nationalists who were chanting racist remarks, sparked a confrontation with an opposing group [3].

A sympathizer of the proceedings drove a car into a crowd of opposing demonstrators, killing one individual and injuring several others. According to the laws of the USA, such violent acts do not qualify as terrorism since hate crimes and murder are not listed as acts of terror. However, the incident illustrates a case of extremism that could potentially contribute to spreading cyber-attacks to a particular agenda [4]. Furthermore, the incident in Charlottesville, Virginia, demonstrates the need to institute changes in the legal system, including federal laws. A clear definition of a criminal act and its punishment facilitates surveil-

lance and monitoring activities to combat such crimes.

The development of information technologies has gradually contributed to the evolution of cyberspace into an environment that strengthens and promotes cyber-atoms in national communication and information systems, thus posing a considerable threat to national security [3]. Depending on the extent of the attack, disruptions in the national systems can contribute to economic losses, damage to resources, and potential access to sensitive data. Hence, the cybersecurity measures adopted help secure electronic information. In addition, the collaboration between individuals, business corporations, and government agencies is necessary to design standards and achieve particular endeavors aimed at fighting activities that endanger the safety of information systems. The mechanisms employed to protect electronic data from unauthorized access should be designed not directly to contribute to cyber espionage.

Strengths and Weaknesses of Literature

Effective measures to ensure cybersecurity have been designed to combat cybercrime. Most of the literature detailed reviews of the factors contributing to the rising cyber threats on critical infrastructure. The increasing dependence on technology, such as the Internet, and the interconnectivity of systems raise the risk of a cyber-attack [9].

Cybercrime perpetrators often exploit vulnerabilities in one system to gain access, disrupt services, and spread terror. Although international terrorist organizations do not conduct most of the cyber-attacks, several cyber-threats are posed by increasing domestic extremism. Different groups have emerged with varying opinions regarding race, political, and religious affairs. Extremist groups such as white supremacists launch a series of cybercrimes to draw attention to their views regarding race. Therefore, the literature identified the escalation of cybercrimes and identified the rising cases of domestic terrorism that largely influence national security.

The studies also provided a clear review of measures that can be employed to promote cybersecurity. For example, the increasing use of digital technologies presents a massive opportunity for individuals, private corporations, and the public sector, including government agencies, to partner to design a robust cybersecurity system [10]. Other measures identified through the evaluation of previous studies include enforcing a reactive and proactive set of criteria to ensure authenticity, confidentiality, integrity, availability, and nonrepudiation of data found in an electronic format. In addition, an automated reporting system was proposed to digitally report suspicious activity on the digital infrastructure by relaying alerts for evaluation and necessary action to ensure the authenticity and integrity of electronic information.

The main weakness identified throughout the reviewed studies includes their failure to address domestic terrorism and the influence of violent extremists spread via the Internet. Domestic terrorist groups use the Internet to recruit

others who share their grievances and ideologies and influence them to commit terror acts against their fellow citizens. These practices must be adequately addressed to ensure cybersecurity and promote national security.

5. Cybersecurity Gaps

The current literature critically analyzes the increasing risks of cyber-attacks and domestic terrorists. For this reason, it also prevents the need for improving cybersecurity to prevent a compromise on national security. However, there are gaps in the current studies that demand evaluation during future research [10].

In short, this includes a limited evaluation of mechanisms used to address domestic terrorism and the inadequate measures that can be used to identify and prevent violent extremists and terrorist groups from influencing young people through the Internet. Once these gaps have been addressed, efficient information sharing between societal organizations and local and federal governments will help combat cyber-attacks and protect electronic data.

6. Future Works: Cybersecurity and Domestic Terrorism

Most cyber-attacks in the United States are perpetrated by domestic terrorist groups guided by varying ideologies, including religious, racial, or politically motivated agendas [10]. Although these attacks do not cause significant damage to critical infrastructure, violent practices against a particular group of people must be identified and stopped. For example, the rising cases of white supremacist conflicts with individuals belonging to other races within the United States should be stemmed out to unify the country. Thus, future work should focus on the mechanisms to address domestic terrorism to reduce cyber threats and other acts of violence. Aside from implementing the available legislation, the focus should be strengthening society against violent extremism. Broad awareness should be done to reduce the threat of targeted violence and terrorism [10].

Further work should promote partnerships with local agencies to facilitate information sharing on potential groups engaging in violent acts based on various ideologies or grievances. Lastly, future research should focus on developing measures to minimize the influence of violent extremists or domestic terrorists online.

Acknowledgements

I want to express my special appreciation to my committee member and Chair, Dr. Ian A. McAndrew, FRAeS, Dean of Doctoral Programs and Engineering Faculty. I am grateful for Dr. McAndrew's timeless support in encouraging my research and writing to continue developing as a scientist and pursuing a third doctorate. Dr. McAndrew's advice on research and academia remains priceless. I would also like to thank Carmit Levin for her enduring support. Furthermore, thanks to my cousin, Ms. Maria Boston, whose academic inputs were invaluable.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Carpenter, N. (2018) The Ad Hoc Federal Crime of Terrorism: Why Congress Must Adequately Amend the Statute to Address Domestic Extremism. *St. John's Law Review*, **92**, 393-418.

[2] Gafni, R. and Pavel, T. (2019) The Invisible Hole of Information on SMB's Cybersecurity. *Online Journal of Applied Knowledge Management* (*OJAKM*), **7**, 14-26. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

[3] Ionita, G.I. (2014) Preliminary Observations on Cybercrime, Cybersecurity, and National Security. *Journal of Public Administration*, *Finance and Law*, 133-139.

[4] Lewis, J.A. (2002) Assessing the Risks of Cyber Terrorism, Cyberwar, and Other Cyber Threats. Center for Strategic & International Studies, Washington, DC.

[5] Osei-Bryson, K.M. and Vogel, D. (2014) Special Issue on Cyber-Security for Development. *Information Technology for Development*, **20**, 93-95. https://doi.org/10.1080/02681102.2014.883115

[6] Shah, A., Ganesan, R. and Jajodia, S. (2019) A Methodology for Ensuring Fair Allocation of CSOC Effort for Alert Investigation. *International Journal of Information Security*, **18**, 199-218. https://doi.org/10.1007/s10207-018-0407-3

[7] Robert, W.T., Eric, J.E. and John, L. (2013) Digital Crime and Digital Terrorism. Pearson Publishing, Dallas.

[8] Taddeo, M. (2019) Is Cybersecurity a Public Good? *Minds and Machines*, **29**, 349-354. https://doi.org/10.1007/s11023-019-09507-5

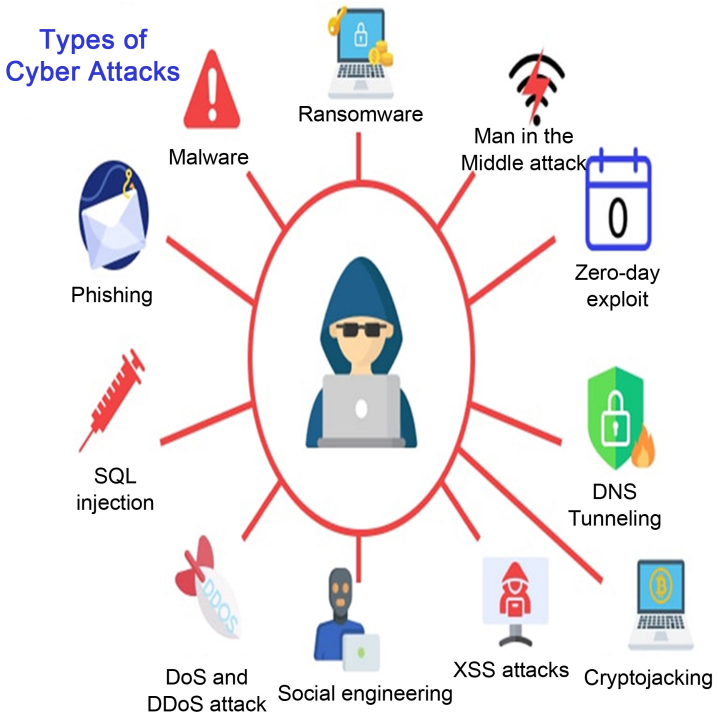
[9] Shank, S. (2011) Cybersecurity: Domestic and Legislative Issues. *American University National Security Law Brief*, **1**, 137-140.

[10] Townsend, R. and Karp, A. (2012) Cyber Security: Defining Cyber Terrorism and Permissible Responses. New York Times.

Appendix A. What Is Cybersecurity?

Note: Adapted from the beginner's guide to cybersecurity (2020, July 13). GW Boot Camps. Retrieved August 23, 2023, from https://bootcamp.cps.gwu.edu/blog/the-beginners-guide-to-cybersecurity/.

Appendix B. Types of Cyber-Attacks



Note: Adapted from What is a cyber-attack? Types and prevention methods (2022). End-to-end API Security for Cloud-Native applications, Wallarm. Retrieved August 23, 2023, from https://www.wallarm.com/what/what-is-a-cyber-attack.