Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector

Abstract:

Currently, the majority of economic, commercial, cultural, social, and governmental activity and contacts between countries, encompassing individuals, non-governmental organizations, and government institutions, occur in the virtual realm known as cyberspace. In recent times, numerous private enterprises and governmental institutions worldwide have encountered the issue of cyber-attacks and the peril associated with wireless communication technology. The modern society heavily relies on electronic technology, and safeguarding this data from cyber-attacks poses a formidable challenge. Cyber-attacks are intended to inflict financial harm onto companies. Cyber-attacks may serve military or political objectives in certain instances. Some examples of these damages include PC infections, knowledge breaches, data distribution service (DDS), and other attack routes. For this purpose, different companies employ diverse strategies to mitigate the harm caused by cyber-attacks. Cybersecurity monitors up-to-date information on the most recent IT data. Researchers worldwide have proposed several techniques to prevent cyber-attacks or mitigate their impact. Several approaches are currently in the operational phase, while others are still in the study phase. The objective of this study is to conduct a thorough examination and evaluation of the latest advancements in the field of cyber security, with the purpose of identifying and analyzing the problems, vulnerabilities, and strengths of the proposed methodologies. A comprehensive analysis is conducted on several forms of novel descendant attacks. The discussion revolves around conventional security frameworks, encompassing their historical context and early-generation approaches to cyber-security. Furthermore, this report presents the latest advancements and developing patterns in the field of cyber security, as well as the current problems and risks to security. The comprehensive review study offered for IT and cyber security researchers is anticipated to be beneficial.

1) Introduction:

In the modern era, the interconnected digital realm known as cyberspace has become an integral component of human existence. With its inception rooted in the development of the internet, cyberspace has rapidly evolved into a dynamic, multifaceted domain that transcends geographical boundaries, facilitating global communication, information dissemination, commerce, and social interactions at an unprecedented scale[1]. This digital ecosystem comprises a complex interplay of networks, technologies, platforms, and virtual environments, shaping the way individuals, organizations, and societies operate, communicate, and perceive reality [2]. The evolution of cyberspace has been marked by transformative technological advancements, from the early stages of computer networking to the current era of cloud computing, artificial intelligence, and the Internet of Things (IoT) [3]. This progression has not only revolutionized the way we access and share information but has also introduced novel challenges and opportunities across various spheres, including cybersecurity, privacy, governance, and socio-cultural dynamics. Understanding the multifaceted nature of cyberspace necessitates an interdisciplinary approach that draws upon fields such as computer science, sociology, psychology, law, economics, and ethics [4]. This research aims to delve into the intricacies of cyberspace, examining its historical development, key technological underpinnings, socio-cultural implications, and the evolving interplay between human behavior and digital environments.

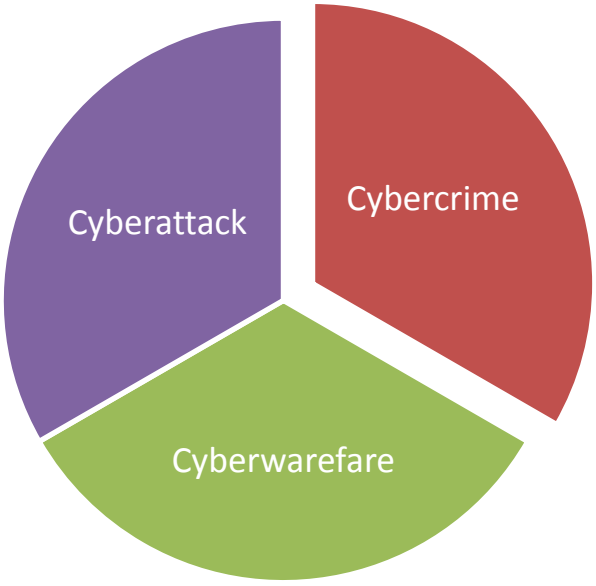

Figure 1 Cyberspace threats

Furthermore, this study seeks to analyze the impact of cyberspace on diverse aspects of contemporary life, including but not limited to:

1. **Cybersecurity and Privacy**: Investigating the challenges and strategies in safeguarding sensitive information, countering cyber threats, and balancing privacy concerns amid the digital landscape's inherent vulnerabilities [5].

2. **Social Dynamics and Identity**: Exploring how online interactions shape social behaviors, identity formation, community structures, and the blurred boundaries between the virtual and physical realms [6].

3. **Economic and Legal Perspectives**: Examining the economic implications of e-commerce, digital currencies, and the legal frameworks governing cyberspace, addressing issues of jurisdiction, intellectual property, and digital rights [7].

4. **Ethical Considerations**: Assessing ethical dilemmas arising from the use of emerging technologies within cyberspace, including AI biases, algorithmic accountability, and the ethical boundaries of virtual reality [8].

1.1) Threat Types:

Cyberspace threats encompass a wide array of malicious activities that can impact individuals, organizations, and governments. Some common threats include [9-19]:

1. **Malware:** Software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, trojans, ransomware, and spyware.
2. **Phishing:** A fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in electronic communication.
3. **DDoS Attacks:** Distributed Denial of Service attacks involve overwhelming a network or server with a flood of internet traffic, causing it to become slow or unavailable to users.
4. **Insider Threats:** This involves threats from individuals within an organization who misuse their access to data, systems, or networks for malicious purposes.
5. **Social Engineering:** Manipulating people into divulging confidential information or performing actions that may compromise security.
6. **Identity Theft:** Stealing someone's personal information to commit fraud or other crimes.
7. **Cyber Espionage:** Illegally acquiring information from individuals, competitors, or governments for strategic, military, political, or economic advantage.
8. **Ransomware:** Malicious software that encrypts a user's data and demands payment, usually in cryptocurrency, for the decryption key.

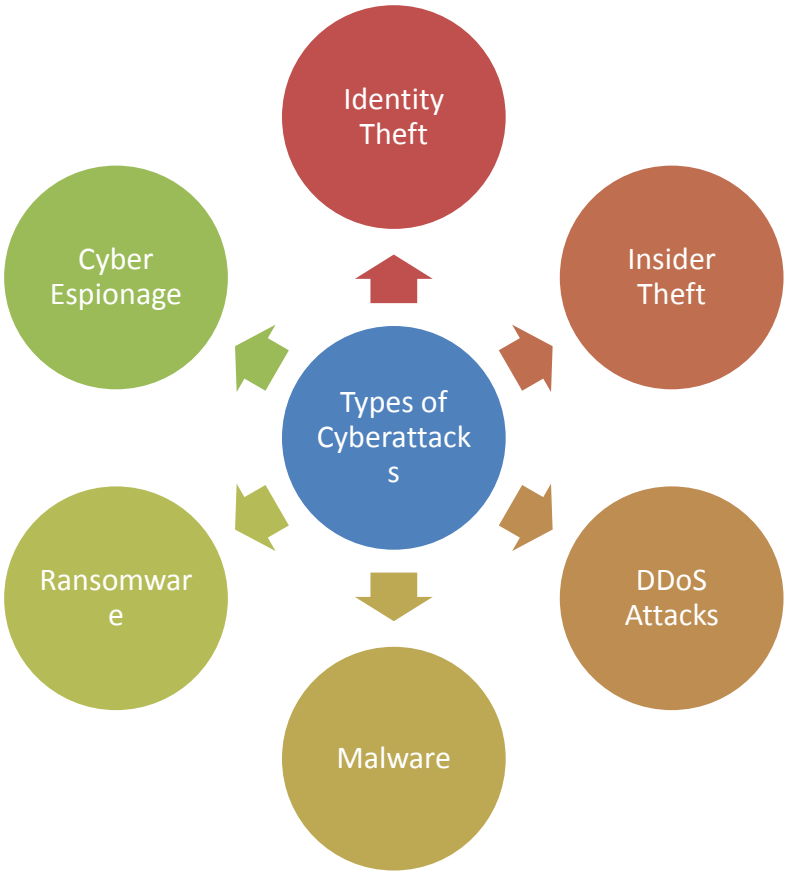

Figure 2Types Of threat

Cyber threats are constantly evolving, and new threats and vulnerabilities emerge regularly. Governments, organizations, and individuals continually work to develop and implement security measures, protocols, and tools to mitigate these threats.

2) Two trends in cybersecuirty:

Two prevailing patterns in the realm of cyberspace:

Consider cyberspace as an expanding balloon that is continuously being inflated. As the balloon expands, its surface area susceptible to a pinprick enlarges, the balloon's skin stretches and becomes thinner, and the trapped air volume increases. The balloon metaphor is employed to elucidate three fundamental aspects of the contemporary cybersecurity landscape:

- Initially, similar to the outer layer of a balloon, the "attack surface area" of cyberspace is continuously growing due to the increasing number of devices being connected to the

internet. Currently, it is estimated that there are billions of devices connected to the Internet, and this number is projected to exceed a trillion during the next decade. Every smartphone, computer, tablet, television, refrigerator, and "intelligent" vehicle has the potential to be targeted by cyber attacks [20].

- Additionally, cybersecurity resources, which are already limited, must strive to keep up with the growing complexity as new devices are introduced and interconnected. By upgrading your outdated home security system to a new one that integrates with your smartphone, you have introduced multiple cyber risks, so complicating the process of safeguarding your house [21, 22].

3) Cyber Space Threats

The expansive nature of the global cyberspace leads to the emergence of overlapping domains of influence, where national entities with varying legal and cultural perspectives and strategic goals exert control [23, 24]. Nations globally have developed a significant reliance on cyberspace for communication and management of the tangible world, to the extent that it is unequivocally impracticable to detach from it. Consequently, the security responsibilities and operations of any nation are progressively influenced by the digital realm [25]. Owing to the worldwide manufacturing of software and hardware goods, it is unfeasible to offer assurances in the product supply chain procedure. The cyber domain's scalability renders it fundamentally distinct. While a bomb's physical range is restricted even under extreme circumstances, cyber-threats have a far broader range of impacts [26, 27]. Consequently, we have implemented a method capable of managing real-world activities. Similar to other domains of knowledge, operations in cyberspace are governed by a relatively limited group of individuals. Users lack the capacity to alter or govern the software and gear they utilize. It is widely acknowledged that only a select few individuals has the ability to properly govern or oversee cyber warfare [28, 29]. Due to the decentralized nature of the cyber world, it is not possible for any one or organization to achieve absolute control, despite the need for intense focus and specialized expertise. The field of cybersecurity undergoes significant changes, driven by the continuous advancement of computing and communication technology [30]. The acceleration is heightened by cyber cohesiveness. Every alteration gives rise to a fresh period of susceptibility and reaction. Cyberspace is highly dynamic and constantly changing [31, 32]. Cyber assets are found in

various organizations, ranging from government-controlled systems to privately held systems. Each institution has varied resources, facilities, capacities, and concerns [33, 34]. Currently, there is a lack of technical capability to accurately attribute activities to specific individuals, groups, or organizations in cyberspace [35]. The primary vulnerabilities in the realm of cyberspace encompass: external threats originating from foreign entities, internal threats arising from within the system, threats stemming from the supply chain of products and services, and risks resulting from inadequate operational capacity of local forces. Foreign intelligence agencies employ cyber technologies to conduct certain aspects of their intelligence collection and espionage operations [36, 37]. There have been many recorded instances globally of the misuse and destruction of a country's information infrastructures, which include computer systems, Internet information networks, and processors and controllers that are essential to important industries [38]. Another source of cyber attacks arises from organized groups who exploit networks for financial gain, and the frequency of these attacks is on the rise.

Figure 3 Sources of Threats

Furthermore, there are instances where other factions (hackers) infiltrate the network to articulate their viewpoints. Presently, it is feasible to penetrate networks with minimal expertise and abilities by acquiring the requisite software and protocols from the Internet and employing them to target other websites. Concurrently, a separate faction known as Hacktivism engages in

politically motivated assaults on well-known websites or email servers. These groups typically place additional burdens on email hosts and, by infiltrating websites, disseminate their political agendas. However, it is important to note that the primary cause of cybercrime within an organization is internal agents who are dissatisfied. These agents do not necessarily require extensive knowledge of cyber-attacks, as their familiarity with the target system often grants them unrestricted access to compromise the system or steal the organization's information. Terrorists pose a significant threat by targeting and attempting to destroy or exploit critical infrastructure in order to undermine national security, cause substantial damage, hurt the economy, and erode public confidence and trust [39, 40].

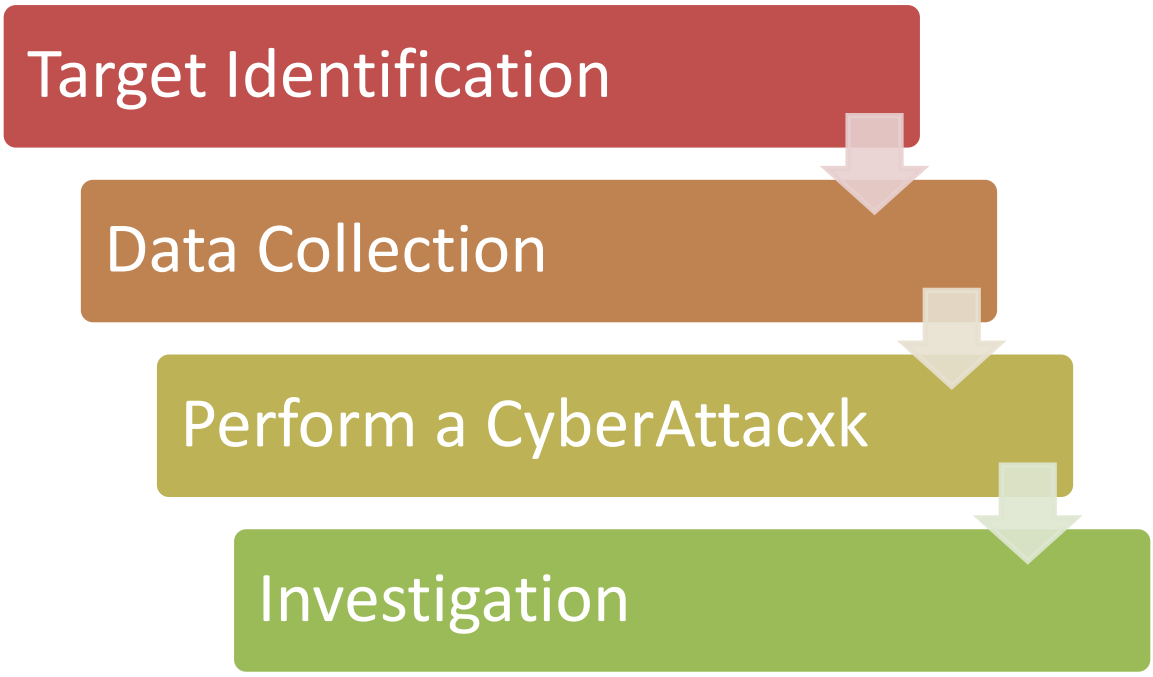

Figure 4 ANATOMY OF CYBERATTACKS

The primary cyber-attack methods include Denial of Service, Logical Bomb, Abuse Tools, Sniffer, Trojan Horse, Virus, Worm, Spamming, and Botnet [41]. The Denial of Service (DoS) method results in the loss of access for both authorized users and the system itself. Indeed, the assailant initiates the process of inundating the target systems with a multitude of messages, so obstructing the lawful transmission of data. This effectively inhibits any system from accessing the Internet or establishing communication with other systems. In an alternative approach known as widespread Denial of Service (DoS), rather than initiating an attack from a single origin, the attackers concurrently target a substantial number of distributed systems. One common method

involves utilizing worms and proliferating them over several computers in order to launch an assault on the intended target [42]. The public has access to abuse tools that can identify and exploit vulnerabilities in networks, catering to various levels of expertise. A logic bomb is a method of attack where a programmer inserts code into a computer that, upon the occurrence of a specified event, triggers the program to carry out a harmful activity. A sniffer is a program that intercepts routed information and analyzes each packet in the data stream to identify specific information, such as passwords [43]. A Trojan horse conceals malicious code and typically masquerades as a benign software that the user willingly executes. Furthermore, a virus contaminates system files, which are often executable applications, by injecting a duplicate of itself into those files. By loading contaminated files into the computer's memory, these versions execute and facilitate the spread of the virus to additional files. Viruses, unlike worms, rely on human interaction in order to spread [44].

4) Cyberthreats In Healthcare Industry:

The advancement of information technologies in the health-care industry not only brings about various beneficial effects, but also exposes it to significant risks posed by entities such as hackers, organized crime, and terrorist organizations. Furthermore, the concurrent proliferation of interconnected devices gives rise to distinct challenges and novel opportunities for exploiting vulnerabilities in the information systems of the diverse entities within the industry. The healthcare industry is consistently confronted with the task of addressing the ever-changing and complex cyber threats. The healthcare sector is highly crucial and need specialised strategies to avoid, detect, and evaluate threats. A recent survey revealed that a minimum of 20% of medical device makers encountered ransomware or malware assaults within the past 20 months [45-47].

Medical devices, such infusion pumps, and healthcare services, such as medicine distribution, have also been specifically targeted by cyber attacks. Implantable cardiac devices are equipped with security measures that are linked to the system architecture. This architecture utilises device-to-device authentication approaches, such as the use of hard-coded credentials on home monitoring devices, to authenticate with patient support networks. An assailant can utilise this authentication information to gain entry into the network [46, 48].

Aside from cyber assaults that exploit vulnerabilities in information technology (IT) infrastructures, social engineering-based attacks are also compromising the security of Healthcare Organisations, often resulting in serious consequences. Malicious actors consistently want to acquire patient-sensitive information, and hacking is widely recognised as a primary factor in the exposure of patient-sensitive healthcare data. Medical IoT devices are now recognised as potential sources of hazards and concerns in the healthcare sector because to their vulnerabilities. More precisely, there have been instances of conducting simulated assaults on various devices, including as pacemakers, insulin pumps, and drug infusion pumps. Malicious software threats like Medjack have the ability to insert harmful code into vulnerable medical equipment, hence affecting other components of the broader healthcare information and communication technology infrastructure. The Centre for Internet Security highlights data breaches, distributed denial-of-service (DDoS) attacks, insider threats, and business email intrusion as the primary cyber attacks in the healthcare sector. A proposal is made for the production and analysis of cyber attack paths to secure the healthcare ecosystem [49-52].

5) Cyberspace And National Security:

Cyberspace has become a critical domain for national security, presenting both opportunities and challenges for policymakers. The implications for national security policy in cyberspace are multifaceted and encompass various dimensions:

1. **Threat Landscape:** The interconnected nature of cyberspace creates vulnerabilities that can be exploited by state and non-state actors. Threats include cyber espionage, cyber warfare, cybercrime, and disinformation campaigns. National security policies need to address these diverse threats and prepare for both known and emerging risks [53].

2. **Defense and Resilience:** Developing robust cybersecurity measures is crucial to defend against cyberattacks. National security policies must prioritize the enhancement of cyber defense capabilities, including investing in secure networks, fostering information sharing among agencies, critical infrastructure protection, and promoting cybersecurity awareness and education [54].

3. **International Relations and Diplomacy:** Cyberspace blurs the traditional boundaries of conflict, raising questions about norms, rules, and laws governing state behavior in this domain. National security policies should engage in international cooperation, negotiations, and agreements to establish norms of responsible state behavior in cyberspace and deterrence strategies against malicious cyber activities [55].

4. **Critical Infrastructure Protection:** Critical infrastructure such as energy grids, financial systems, and healthcare facilities are increasingly reliant on networked systems, making them prime targets for cyber threats. National security policies need to prioritize protecting and securing these critical assets through regulations, standards, and investments in cybersecurity [56].

5. **Military and Strategic Considerations:** Cyberspace has become a domain for military operations alongside land, air, sea, and space. National security policies must consider integrating cyber capabilities into military strategies, including offensive and defensive cyber operations, to maintain a credible deterrent and response capability [57].

6. **Intelligence and Surveillance:** Cyberspace offers opportunities for intelligence gathering but also presents challenges due to the vast amount of data and the need to differentiate between legitimate and malicious activities. National security policies need to balance intelligence collection with privacy concerns and legal frameworks [58].

7. **Public-Private Partnerships:** Collaboration between government agencies, private sector entities, and academia is essential to address cyber threats effectively. National security policies should foster public-private partnerships to leverage expertise, resources, and innovation in developing cybersecurity solutions [59].

8. **Cyber Talent and Education:** A skilled workforce is crucial to defend against cyber threats. National security policies should focus on promoting cyber education, training cybersecurity professionals, and attracting talent to work in government agencies and the private sector [60].

In summary, developing comprehensive and adaptive national security policies that recognize the complexities and dynamic nature of cyberspace is critical to safeguarding a nation's interests,

infrastructure, and citizens in the digital age. Constant evaluation, adaptation, and collaboration are necessary to stay ahead in the evolving landscape of cyber threats and opportunities.

6) The Way Ahead; Future Perspectives:

In order to enhance the cybersecurity of this nation and effectively address emerging threats, it is imperative to consistently pursue two primary objectives [61]:

• Initially, facilitate significantly enhanced dissemination of information and cooperation among crucial departments and agencies (Department of Justice, Department of Homeland Security, Department of Defense, and Office of the Director of National Intelligence) as well as the private sector. The Cybersecurity Information Sharing Act of 2015 was a necessary, albeit cautious, measure aimed at promoting the sharing of information between the private sector and the U.S. government regarding cybersecurity threats. This includes the exchange of classified vulnerabilities, best practices, and defensive measures, facilitated by liability protections. This legislation could enhance the community's ability to anticipate attacks and adopt a more proactive defense stance.

• Secondly, establish a state of collaboration and coordination throughout the entirety of the United States government. Currently, several governmental entities own distinct cyber obligations. This concept is highly logical and valid due to the fact that various agencies possess distinct capabilities, hence they should be assigned tasks that align with their respective areas of expertise. The key is to effectively utilize all the capabilities towards a shared objective, and that is where the challenge arises. Effective cyber protection necessitates a well-organized and unified reaction, but the current bureaucratic obligations impede advancements towards achieving this objective. President Obama's designation of a Chief Information Security Officer for the Ultimately, the ideal solution is to possess the capability to monitor and trace cyber invaders, criminals, and other hostile individuals in cyberspace with the same level of agility and swiftness as these enemies possess. Attaining this objective will necessitate a consistent and enduring endeavor over an extended period.

The implementation of new regulations will necessitate the establishment of additional governing bodies, as well as extensive modifications to the U.S. Code (a formidable

undertaking). There will be a spirited public debate. Undoubtedly, I have consistently maintained that public discourse is an essential initial phase: The intervention of the government into private issues, even for the sake of protecting the public, elicits an emotional reaction. . . . An initial measure necessitates a candid and open discussion that challenges the fundamental barriers between the public and private sectors, which are essential to democracy. Moreover, it is imperative to engage in a discourse on the optimal approach to striking a balance between the imperative of security and the preservation of privacy. There exist other methods to enable this type of conversation, and the suggestion presented by Full Committee Chairman Michael McCaul and Senator Mark Warner is a potential approach to progress, although alternative options may also be available. It is reasonable to state that the current debate on the obligation of device manufacturers to incorporate "backdoors" into operating systems, enabling law enforcement and intelligence services to gather data, has initiated a crucial conversation. This is a positive aspect. In the immediate future, the subsequent actions will be multifaceted. Congress should persist in formulating robust and intelligent rules and legislation aimed at enhancing cybersecurity, such as the Cybersecurity Information Sharing Act of 2015. While there is an urgent requirement for these policies and legislation, it would be prudent for Congress to gradually formulate and disseminate them to instill public trust in the government's competence and motives. Convincing the public that the government's information requirements are in equilibrium with people' privacy preferences is crucial. Currently, numerous concepts and methodologies for utilizing technology to enhance cybersecurity, such as aggregating and analyzing extensive data repositories, cause concern among individuals who advocate for the right to privacy and oppose government interference. It is important to recognize that every individual has a responsibility to contribute to the enhancement of cybersecurity [62-69].

The U.S. government should persist in promoting and fostering the exchange of information and collaboration between government entities and the private sector to safeguard citizens, businesses, and vital infrastructure against cyberthreats. The Secretary of the Department of Homeland Security, Jeh Johnson, has recently released initial guidelines for the exchange of information between the private sector and the United States government. In due course, the U.S. government should likewise endeavor to utilize all types of data and intelligence to detect and predict both dangers and malicious individuals, while respecting individuals' privacy preferences to an acceptable extent [70, 71].

• Individuals and organizations involved in the creation and distribution of Internet-connected software and hardware, ranging from huge enterprises to individual app developers, must possess the knowledge and skills to comprehend the security implications of their work. Currently, a software developer is not required to possess a degree, formal training, or any license in order to create programs that manage our infrastructure. Very few engineering domains have the same dilemma, if any at all. For instance, the construction of a drawbridge necessitates the supervision and endorsement of a certified civil engineer, yet theoretically, anyone can build the software that governs the operation of that bridge. Ensuring cybersecurity is a collective duty, spanning from the chief information security officer to the individual app developer [72, 73].

• It is imperative for individual customers to take further measures to safeguard their software, hardware, and confidential data. In essence, the majority of individuals are either excessively occupied or inadequately trained (probably both) to dedicate their time and effort to fixing every equipment in their household. We frequently maintain outdated and inherently insecure equipment and computers in operational condition. According to the Cybersecurity National Action Plan issued by the President, there is a significant presence of antiquated and obsolete devices connected to the internet. This situation creates vulnerable access points that can be readily exploited and utilized as "botnet soldiers" [74, 75].

Conclusions:

The third century recognizes cyberspace and its associated technologies as a paramount source of power. The attributes of cyberspace, including affordable access, anonymity, susceptibility, and imbalance, have given rise to the phenomenon of power diffusion. This implies that while governments have traditionally monopolized power, it is now being shared with other entities such as private corporations, organized terrorist and criminal factions, and individuals. However, governments still retain a significant role in this dynamic. Undoubtedly, this occurrence will not compromise the national security of states. The evaluation of this effect can be conducted using many methods. The first aspect to consider is the notion of security. The concept of national security has evolved beyond military concerns and territorial boundaries. Presently, the deteriorating quality of life experienced by citizens poses a significant danger to national security. An additional aspect is the eradication of the spatial component of cyber threats.

Historically, military threats were confined to a certain geographic area. Hence, it was quite effortless to handle, particularly when it came to recognition. The third factor to consider is the magnitude of risks presented by cyber attacks. These threats occur irregularly, have multiple dimensions, and because to their association with important networks and infrastructure, they can cause significant harm. Furthermore, conventional methods like military and police force are insufficient to contain these threats. Governments alone are also inadequate in countering them. What is needed is a combination of effective collaboration between governments and the private sector, as they both share a vested interest in addressing these challenges. He demands in the face of such threats. Furthermore, it is important to note that cyber dangers extend beyond governmental entities, posing risks to both individuals and corporations, leaving them vulnerable to the detrimental consequences of such threats. Furthermore, the ideas in international relations that are largely focused on government may be easily disregarded or perplexing, as security in the digital age extends beyond the realm of government alone.

References:

1. *M.R. Shad, Cyber threat in interstate relations: case of US-Russia cyber tensions. Policy Perspect. 15(2), 41–55 (2018).*
2. *D. Sarathchandra, K. Haltinner, N. Lichtenberg, College students' cybersecurity risk perceptions, awareness, and practices, in 2016 Cybersecurity Symposium (CYBERSEC) (IEEE, 2016), pp. 68–73.*
3. *F. Mouton, L. Leenen, H.S. Venter, Social engineering attack examples, templates and scenarios. Comput. Secur. 59, 186–209 (2016).*
4. *D. Kahneman, Thinking, Fast and Slow (Penguin Books, 2011).*
5. *Z.L. Švehla, I. Sedinić, L. Pauk, Going white hat: Security check by hacking employees using social engineering techniques, in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (IEEE, 2016), pp. 1419–1422.*
6. *S. Uebelacker, S. Quiel, The social engineering personality framework, in 2014 Workshop on Socio-Technical Aspects in Security and Trust (IEEE, 2014), pp. 24–30.*
7. *A.S. Alazri, The awareness of social engineering in information revolution: techniques and challenges, in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (IEEE, pp. 198–201) (2015).*
8. *G.L. Orgill, G.W. Romney, M.G. Bailey, P.M. Orgill, The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, in Proceedings of the 5th Conference on Information Technology Education (2004), pp. 177–181.*
9. *I. Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh, Social engineering attack strategies and defence approaches, in 2016 IEEE 4th International Conference on Future internet of Things and Cloud (FiCloud) (IEEE, 2016), pp. 145–149.*
10. *C. Hadnagy, Social Engineering: The Art of Human Hacking (Wiley, 2010).*

11. *A. Berg, Cracking a social engineer. Comput. Secur. 8(14), 700 (1995).*
12. *K.W. Mahmoud, Cyber Attacks: The Electronic Battlefield (Arab Center for Research and Policy Studies, 2013). http://www.jstor.org/stable/resrep12651. Last accessed on 21 Nov 2021.*
13. *J.S. Nye, Nuclear lessons for cyber security? Strateg. Stud. Quart. 5(4), 18–38 (2011).*
14. *S. Timothy et al., Countering cyber war, NATO Rev. (2001). https://www.nato.int/docu/review/articles/2001/12/01/countering-cyber-war/index.html. Last accessed on 25 Oct 2021.*
15. *N. Melzer, Cyberwarfare and International Law (UNIDIR Resources, 2011). https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Last accessed on 22 Nov 2021.*
16. *Commonwealth of Australia, Defence White Paper 2013 (Canberra Department of Defence 2013).*
17. *A.-M. Taliharm, Towards Cyberspace: Managing Cyber War Through International Collaboration. https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwarthrough-international-cooperation. Last accessed on 26 Nov 2021.*
18. *I. Mann, Hacking the Human: Social Engineering Techniques and Security Countermeasures (Routledge, 2017).*
19. *J. Goodchild, Social engineering: the basics. CSO Online (2012).*
20. *K. Krombholz, H. Hobel, M. Huber, E. Weippl, Advanced social engineering attacks. J. Inf. Secur. Appl. 22, 113–122 (2015).*
21. *M.M. Singh, S.S. Siang, O.Y. San, N. Hashimah, A.H. Malim, A.R.M. Shariff, Security attacks taxonomy on bring your own devices (BYOD) model. Int. J. Mob. Netw. Commun. Telemat. (IJMNCT) 4, 117 (2014).*
22. *A.G. Bello, D. Murray, J. Armarego, A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. Inf. Comput. Secur. (2017).*
23. *M.R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, N. Kaabouch, Social engineering attacks a reconnaissance synthesis analysis, in 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (IEEE, 2020), pp. 0843–0848.*
24. *J.W. Bullée, L. Montoya, M. Junger, P.H. Hartel, Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention, in Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016 (IOS Press, 2016), pp. 107–114.*
25. *D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, C. Pu, Reverse social engineering attacks in online social networks, in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (Springer, Berlin, Heidelberg, 2011), pp. 55–74.*
26. *E. Blancaflor, C.V.H. Banzon, C.J.J. Jackson, J.N. Jamena, J. Miraflores, L.K. Samala, Risk assessments of social engineering attacks and set controls in an online education environment, in 2021 3rd International Conference on Modern Educational Technology (2021), pp. 69–74.*
27. *N.Y. Conteh, P.J. Schmick, Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int. J. Adv. Comput. Res. 6(23), 31 (2016).*
28. Aldawood, H. and G. Skinner, *Contemporary cyber security social engineering solutions, measures, policies, tools and applications: a critical appraisal.* Int. J. Secur. (IJS), 2019. **10**.
29. *Lun, Y.Z.; et al.: Cyber-physical systems security: a systematic mapping study. arXiv:1605.09641 (2016).*
30. *Razzaq, A.; et al.: Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). IEEE (2013).*
31. *Bada, M.; Sasse, A.M.; Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? arXiv:1901.02672 (2019).*

32. *Floyd, D.H.; Shelton, J.W.; Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. Google Patents (2018).*
33. *Ron, M.: Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In: Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018). Springer (2018).*
34. *Mittal, S.; et al.: Cybertwitter: using twitter to generate alerts for cybersecurity threats and vulnerabilities. In: Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. IEEE Press (2016).*
35. *Kustarz, C.: et al.: System and method for denial of service attack mitigation using cloud services. Google Patents (2016).*
36. *Niemelä, J.; Hyppönen, M.; Kangas, S.: Malware protection. Google Patents (2016).*
37. *Choraś, M.; et al.: Correlation approach for SQL injection attacks detection. In: International Joint Conference CISIS'12-ICEUTE´12-SOCO´12 Special Sessions. Springer (2013).*
38. *Gill, R.S.; Smith, J.; Looi, M.H.; Clark, A.J.: Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks. In: Clark, A.J., Kerr, K., Mohay, G.M. (eds.) AusCERT Asia Pacific Information Technology Security Conference: Refereed R&D Stream, 22–26 May 2005, Gold Coast, Australia (2005).*
39. *Wassermann, G.; Su, Z.: Static detection of cross-site scripting vulnerabilities. In: Proceedings of the 30th International Conference on Software Engineering. ACM (2008).*
40. *Kieyzun, A.; et al.: Automatic creation of SQL injection and cross-site scripting attacks. In: Proceedings of the 31st International Conference on Software Engineering. IEEE Computer Society (2009).*
41. *Muccini, H.; Sharaf, M.; Weyns, D.:. Self-adaptation for cyber-physical systems: a systematic literature review. In: Proceedings of the 11th International Symposium on Software Engineering for Adaptive and Self-managing Systems. ACM (2016).*
42. *Chockalingam, S.; et al.: Bayesian network models in cyber security: a systematic review. In: Nordic Conference on Secure IT Systems. Springer (2017).*
43. *Budgen, D.; Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceedings of the 28th International Conference on Software Engineering. ACM (2006).*
44. *Kitchenham, B.A.; Budgen, D.; Brereton, O.P.: The value of mapping studies-A participant-observer case study. In: EASE (2010).*
45. *Microsoft. Stride model (2022). https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model. Accessed 22 Sept 2023.*
46. *Tikhomirov, M., Loukachevitch, N.V., Sirotina, A., Dobrov, B.V.: Using BERT and augmentation in named entity recognition for cybersecurity domain. In: Natural Language Processing and Information Systems—25th International Conference on Applications of Natural Language to Information Systems, NLDB 2020, vol. 12089, pp. 16–24. Springer, Saarbrücken, Germany (2020). https://doi.org/10.1007/978-3-030-51310-8_2.*
47. *Institute, P.: Sixth annual benchmark study on privacy & security of healthcare data. Tech. rep, Ponemon Institute (2016).*
48. Aghaei, E., et al., *Securebert: a domain-specific language model for cybersecurity*, in *Secur. Privacy Commun. Netw.*, F. Li, et al., Editors. 2023, Springer: Cham.
49. Alwaheidi, S. and M.K.S. Islam, *Data-driven threat analysis for ensuring security in cloud enabled systems.* Sensors, 2022. **22**.
50. Ameri, K., et al., *Design of a novel information system for semi-automated management of cybersecurity in industrial control systems.* ACM Trans. Manag. Inf. Syst., 2023. **14**.

51. Aracri, G., A. Folino, and S. Silvestri, *Integrated use of KOS and deep learning for data set annotation in tourism domain.* J. Doc., 2023.
52. Silvestri, S., et al., *A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem.* Sensors, 2023. **23**.
53. *Chong, R.: Quick reference guide to endnote (2018).*
54. Abomhara, M. and G.M. Køien, *Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks.* J. Cyber Secur., 2015. **4**.
55. Al Mazari, A., *Cyber terrorism taxonomies: definition, targets, patterns, risk factors, and mitigation strategies*, in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. 2018, IGI Global: Hershey.
56. Alguliyev, R., Y. Imamverdiyev, and L. Sukhostat, *Cyber-physical systems and their security issues.* Comput. Ind., 2018. **100**.
57. Banks, W.C., *Cyber espionage and electronic surveillance: beyond the media coverage.* Emory L. J., 2016. **66**.
58. Beecham, S., *Using an expert panel to validate a requirements process improvement model.* J. Syst. Softw., 2005. **76**.
59. Benedickt, M., *Cyberspace: First Steps*. 1991, Cambridge: MIT Press.
60. Benson, V., J. McAlaney, and L.A. Frumkin, *Emerging threats for the human element and countermeasures in current cyber security landscape*, in *Psychological and Behavioral Examinations in Cyber Security*. 2018, IGI Global: Hershey.
61. Brar, H.S. and G. Kumar, *Cybercrimes: a proposed taxonomy and challenges.* J. Comput. Netw. Commun., 2018. **2018**.
62. Choo, K.K.R., *The cyber threat landscape: challenges and future research directions.* Comput. Secur., 2011. **30**.
63. Dodge, R.C., C. Carver, and A.J. Ferguson, *Phishing for user security awareness.* Comput. Secur., 2007. **26**.
64. Enoch, S.Y., *A systematic evaluation of cybersecurity metrics for dynamic networks.* Comput. Netw., 2018. **144**.
65. Franke, U. and J. Brynielsson, *Cyber situational awareness—a systematic review of the literature.* Comput. Secur., 2014. **46**.
66. Gunkel, D.J., *Hacking Cyberspace*. 2018, Abingdon: Routledge.
67. Hansen, L. and H. Nissenbaum, *Digital disaster, cyber security, and the Copenhagen School.* Int. Stud. Q., 2009. **53**.
68. Hydara, I., *Current state of research on cross-site scripting (XSS)—a systematic literature review.* Inf. Softw. Technol., 2015. **58**.
69. Johnson, C., *Guide to cyber threat information sharing.* NIST Spec. Publ., 2016. **800**.
70. Kuehl, D.T., *From cyberspace to cyberpower: Defining the problem*, in *Cyberpower and National Security*. 2009, National Defense University Press: Washington, D.C.
71. Lewis, G. and P. Lago, *Architectural tactics for cyber-foraging: results of a systematic literature review.* J. Syst. Softw., 2015. **107**.
72. Mishna, F., *Interventions to prevent and reduce cyber abuse of youth: a systematic review.* Res. Soc. Work Pract., 2011. **21**.
73. Mohammed, N.M., *Exploring software security approaches in software development lifecycle: a systematic mapping study.* Comput. Stand. Interfaces, 2017. **50**.
74. Mufti, Y., *A readiness model for security requirements engineering.* IEEE Access, 2018. **6**.
75. Nguyen, P.H., S. Ali, and T. Yue, *Model-based security engineering for cyber-physical systems: a systematic mapping study.* Inf. Softw. Technol., 2017. **83**.