"A The Professionalization Of The Hacker Industry Using Mathematics"

Abhay Kumar Mishra[1*], **Dr. Kk Sen**[2]

[1*]Assistant Professor Department Of Computer Science, Shri Rama Krishna College Of Engineering Science And Management. mishraabhay87srist@gmail.com
[2]Assistant Professor Department Of Mathematics, Shri Rama Krishna College Of Engineering Science And Management. Krishnakumarsen8@gmail.com

ABSTRACT:
The Internet and other internationally networked infrastructures used to provide information services are indispensable to society. An unprecedented demand for information access has been brought about by the development of information technology (IT) and information systems (IS) over the past few decades. The consequence of wireless mobility are immense, and the business possibilities of new and inventive wireless flexibility are just beginning to be realized with the rise of the Internet of Things (IOT). The history of hacking and the professionalization of the hacker industry are examined in this essay. The hacker business is become increasingly adaptable and adaptive as it gets more fully professionalized, making it more difficult for law enforcement and intelligence to combat. Additionally, the hacker industry is making it harder to distinguish between motivated crime and more conventional computer security risks, such as network intrusion or the destruction of vital infrastructures.

KEY WORD: social network soft ware, mathematics function and matrix, differential and integral.

INTRODUCTION:

Hacking what has been the most significant development in computing during the past few decades? Despite the headlines, the most noteworthy emerging trend may not be the dotcom bubble's collapse, Google's subsequent hegemony, or even the emergence of Web 2.0 and social networking apps like Twitter and Face book [i.e., Meta]. Instead, the Internet of Things (IoT) and the development of a professional hacker "industry" that is both global in reach and diverse at the local and regional level may be the most significant computing developments of the past ten years. ransom ware, malicious software (malware), and cybercrime, which are the products of this sector, not only pose a direct and indirect threat to the national security of the United States, but they also run the risk of jeopardizing the Internet's integrity as a platform for commerce and communications. Although the US government and media have acknowledged the threat posed by hacking, government representatives and security companies have mostly spoken about it in technical terms up to this point. This article aims to discuss the rise and diversification of the hacker as part of a broader attempt by security professionals to comprehend the global cultures of hackers. Some of the biggest, most advanced, and most serious cyberattacks in recent years have included WannaCry [48], the Equifax data breach [35], and the Facebook data leak [44]. This has an impact on thousands of enterprises, government agencies, and millions of customers. The word "hacking" has many different meanings for American audiences, from the favorable ones connected to the open-source software movement to the prevalent perception of hackers as "cyberpunk" criminals [3]. These linkages, which are a holdover from the early days of hacking in the US, run the risk of deceiving analysts about the kind of people who become hackers as well as the global nature of modern hacking [24].

The stereotype of the hacker as a nerdy young guy or girl in a black hoodie, causing computer trouble in the basement of his parents' suburban home, must be set aside when considering the diversity of people who participate in hacking. This misconception not only misrepresents the culture of even American hackers, but it also ignores how different hacker cultures are among nations and regions (International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 3, June 2022 88). On the other hand, in a society where information is a highly prized resource,

Many people will take drastic steps to either steal or defend this information. The Internet, a global network of networks, offers amazing access to a tremendous amount of data and information, facilitating connection like never before. However, this same interconnectedness also gives others the ability to monitor communications and obtain information without the required authority. Information security was not as important to the Internet's architecture as interoperability and interconnection [14]. As a result, hackers—those who break into computers and computer networks with the intent to cause harm—can maliciously affect these systems, infrastructures, and human behavior [33].

There are two types of malicious activities that might occur: (1) destructive attacks, and (2) non-destructive network exploitation, which is the employment of methods, usually covert, to obtain unwanted access, mainly to steal data from a network [39]. Even amateurs can infiltrate and misuse a network or its users due to the accessibility of hacking information and the simplicity with which unlawful activities can be carried out. Security experts have found this duality problematic, and hackers take advantage of it.

The hacker industry is making it harder to distinguish between motivated crime and more conventional computer security risks, such as network intrusion or the destruction of vital infrastructures. Numerous cyber events have occurred in the past, including assaults against foreign ministries, defense contractors, and government employees1. According to the Ponemon Institute's 2021 Cost of Data Breach Report, which was sponsored by IBM, the average cost of a data breach increased from $3.86 million in 2020 to $4.24 million in 2021. $3. The average cost of a ransomware breach was $4.62 million, the average cost of a breach in hybrid cloud environments was 61 million, and the formalization and commercialization of the hacker industry is creating networks and tools that, although intended for use against governments or corporations, can also be used to target individuals [31, 40]. The same methods and tools that are used to hack into wired systems for identity theft, fraud, or intellectual property theft can be quickly redeployed to engage in IoT networks as well [26]. In conclusion, the IoT network is facilitating a previously unheard-of new cybercrime.

since high levels of transparency, a lack of security configurations when in use, and privacy concerns make IoT devices typically susceptible to security threats [11]. British tech pioneer Kevin Ashton, Executive Director of AutoID Labs at MIT, didn't use the term "Internet of Things" until 1999 in order to draw attention to a fascinating new technology known as radio frequency identification (RFID).3. The Internet of Things is continually growing to accommodate the introduction of rapidly evolving technologies and methods of access (such as cloud computing, edge computing, microservices, etc.), communications, as well as new smart gadgets (such cellphones, sensors, readers, tags, etc.). Technical push for greater and ever-increasing connectedness. 89 immediate and broader environment: the environment as an interface [34] is a logical extension of the computing capability in a single machine to the environment. Because these devices aren't set up for security, exploitation gets easier as the IoT transmission network gets easier to connect to. Newer and more potent technologies brought about by widespread interconnection might not always satisfy the certification and dependability requirements of an IoT provider [6]. Due to these shifting market dynamics, there is now a chance for an unintentional or intentional disruption. Unproven technologies and inexperienced carriers create interconnection hazards. IoT network technologies, such mobile data and Internet protocol-based networks, have become conduits for important transaction traffic and hosted information, giving hackers more opportunity to take advantage of these opportunities [33]. IoT networks are open to new areas of illegal activity as more and more of these devices connect to the Internet. In consequence, new security tools and techniques will be required for efficient security defense as IoT networks grow more diverse and complicated than those used now.

A HACKING HISTORY:

In order to make itself accessible to everyone, the Internet has developed into an open global network that unifies all computer networks worldwide. Information sharing among computer users has been made possible by the Internet, but it has also resulted in negative phenomena including computer viruses, pornographic content, unauthorized access attempts, theft of private data, and internal data corruption [14]. In addition to having a wide variety of assault tools, computer "hackers" nowadays have perfected extremely intricate evasion and stealth strategies that allow them virtually unrestricted access to the Internet [35]. Since the late 1950s, hacking has been practiced in a variety of ways [29]. In the modern computer and IT business, the term "hacker" has two meanings. The word was first defined by researchers as [43]: Hacker noun 1. Unlike most computer users, who would rather learn the bare minimum required, this individual enjoys knowing the ins and outs of computer systems and how to maximize their potential. 2. Someone who appreciates or is passionate about programming as opposed to merely theorizing about it. The term 'hacker' was coined in the late 1950s to describe computer specialists in academic contexts. The phrase "hack" was first used at the Massachusetts Institute of Technology (MIT) to refer to a sophisticated, clever, or creative method of making computers operate significantly more efficiently [25]. Most people agree that these early 'old school' hackers from the 1950s and 1960s were the forerunners of the contemporary computer underground [19]. The early generations of hackers pioneered public access by fervently pursuing computers and computer systems that were intended to be practical and available to individuals [38, 42, 21]. During this time, computer programmers believed that their work was groundbreaking since it challenged established computer science concepts [29]. The transfer of computers from academia to the military in the early 1960s infuriated programmers. Secrecy meant freedom to share code in the computer lab, collaboration in program design, and the power to change everything and everything depending on one's own skill to make it better to the hackers of the 1960s [39]. During this period, hackers started to develop a set of principles and values known as "hacker ethics," which were defined as follows: All information ought to be freely accessible; authorities ought to be distrusted; decentralization ought to be encouraged; hackers ought to be evaluated on the basis of their hacking rather than on false standards like degrees, age, race, or status; Computers can improve your life, and they can be used to create art and beauty [38].

The criminal hacker gained popularity in the 1970s. The formation of the Youth International Party (YIP) to engage in political mischief and surrealistic subversion, the encouragement of phreaking4 to steal money from capitalist phone companies, and the establishment of the Technical Assistance Program (TAP) to freely disseminate information through the technical aspects of telephony were all products of the counterculture of this era [29]. In order to connect the first hackers online, the first electronic bulletin board systems (BBS) are developed during this period [18]. The BBS was a computer system that served as a sort of community center or open forum, typically operated from a hacker's house [18]. BBS conversation was mostly about computers and electronics at the time, and the majority of people with access to computers and modems were programmers or scientists.

The illegal commerce in pirated software was one of the many new subjects and applications that BBS covered. The idea of the 'new-school' hacker as a criminal was cemented in the 1980s. The popularity of the personal computer (PC) raises the number of BBS and modem users as well as the potential hacker population [28]. Hacking organizations like the Masters of Deception (USA), the Legion of Doom/Hackers (USA), and the Chaos Computer Club (Germany) create and participate in bold and well-known computer intrusions such phone line jamming and online warfare [11]. The movie "WarGames" exposes the audience to hacking and illustrates the possible danger that comes with youngsters using computers [31]. At a startling rate, Robert Morris spreads the first self-replicating Internet worm (such as the computer virus) over the country's computer networks [29]. The media took notice of the exploits of two hackers, Kevin Mitnick5 and Kevin Lee Pouslen, who were both apprehended, charged, and imprisoned for their telephone hacking [39].

An initial Legion of Doom member, The Mentor, produces "The Hacker Manifesto," which vividly depicts the hacker's attitude toward technology, separating them from the rest of society and dividing the hacker subculture [39]. As a result of these incidents, Congress passed the Computer Fraud and Abuse Acts in 19866 and started to label hacking as abnormal.

The number of online users and prospective targets skyrocketed in the 1990s as a result of the Internet's inception. The movie 'Hackers' spawned a second generation of hackers and drew in a fresh wave of tech-savvy hackers who viewed the Internet as the next frontier to be explored [19]. Russian hackers target the FBI and Pentagon websites and steal $10 million from Citibank [11]. The government of the United States cracks down hard on hacking groups [16]. Hacker activity and computer portability were altered by the rise of laptops and Wi-Fi [41].

The connectivity between hacker communities has grown since the start of the twenty-first century due to the globalization of technology and the Internet. As hacking threats increase, so does the safeguarding of critical infrastructure [18]. Advanced hacks like Titan Rain7 and the TJX8 show how dangerous the hacker community is becoming [24]. Organizations like Shadowcrew [13] and the Russian Business Network [6] show how professional and widespread the hacking industry is.

Up until the early 2000s, the majority of hackers were essentially amateurs driven mostly by curiosity, a desire for recognition or celebrity, or a desire to further a social or political cause (i.e., hacktivism) [47]. Although these motivations are undoubtedly still there, the massive rise in financially motivated cybercrime in recent years has outweighed them [43]. Hacking has transformed from a niche pastime of thrill-seeking, glory-seeking geeks to a profitable industry that adopts a strict, disciplined approach to creativity and execution [37]. The exact extent of the hacking industry is unknown, as is the case with all illicit economies. According to some analysts, the global market for hacking tools including bots, adware, malware, and other types of cybercrime costs the US economy more than $100 billion annually, albeit estimates should be regarded with caution [27]. There is no doubt that the market's value is increasing quickly and getting increasingly complex. Over the past 20 years, there have been numerous instances of IoT-connected devices being compromised [10, 16, 22]. For instance, The July 2015 Jeep breach was discovered by an IBM security intelligence report after a group of researchers used the controller area network (CAN bus) of a Jeep SUV to gain complete control of the vehicle [7]. They gained control of the car via the Sprint cellular network by taking advantage of a firmware update vulnerability, and they found that they could cause it to accelerate, decelerate, and even swerve [7]. An IoT botnet using malware dubbed Mirai was used to perform the largest distributed denial-of-service (DDoS) attack ever against service provider Dyn in October 2016, one of the first reported IoT attacks against the commercial sector [45]. Large chunks of the Internet, including CNN, Reddit, Netflix, Twitter, and the Guardian, went down as a result. The FDA acknowledged in early 2016 that St. Jude Medical's implantable cardiac devices had security flaws that hackers could use to get access to the devices [2]. The hacker might alter the gadget's pace, drain the battery, and even shock the patient once they have control of the device [2]. Supply chains [47], ICS/SCADA systems [17,39], hospitals [23], water treatment systems [19], the Colonial Pipeline [7], and numerous other businesses [1] have been the targets of numerous ransomware IoT assaults in recent years.

The IoT hacker industry's growing array of goods and services, which aim to lower operational risks and boost profit margins, has been a crucial component of the sector. The variety of attacks offered by the IoT hacker community has not changed in the past ten years [39,27]. Intellectual property (IP) and identity theft, spamming, phishing, and denial-of-service (DoS) assaults have replaced self-propagated worms and hard-drive eating viruses, which were the main worries in the late 1990s and early 2000s [8, 15]. IoT botnets, which can be deployed for a number of reasons, have made this transition easier. - spamming, DoS, selfreplication, cyberwarfare, etc. [20]. Innovation in the IoT hacker industry focuses as much on "social engineering" as on discovering new technical exploits [11]. Hackers are seeking for the easiest rather than the cleverest point of access into systems. Society is still striving to come to grips with this new criminal conduct that knows no geographical limits and blurs the idea of criminal jurisdiction [20, 28, 34]. Research on hacking and hackers has concentrated on subjects such application and system programming [4], software piracy [20, 22], hackers' ethics [17, 32], and cognitive hacking [19, 27]. Furthermore, the majority of research on hackers has been carried out by practitioners, such as consultants, researchers, or IT specialists; frequently, these studies have relied primarily on a single interview or proxy populations rather than actual hackers [29, 35]. The state of research on wireless network hacking is a little more developed. Hacking wireless systems is the subject of numerous technical investigations, such as those published in [11, 26, 36]. The study provides empirical support for the reasons ethical hackers provide for breaking into information systems and provides guidance on how to mitigate the issue.

A perceived technical challenge, a need for peer recognition, and a desire to inform others about security vulnerabilities are some of the reasons given for hacking [30, 16]. Computer networks and their services are prone to weaknesses, as history has demonstrated; security issues are present in all telecommunications services, including those provided by the Internet of Things. Since each IoT network is different and its components serve different purposes, various security measures need to be put in place. On the other hand, one may argue that IoT networks are much more susceptible to hacking risks than conventional wireless networks. Even though network security gets better with every new technology generation, the Internet of Things will still face challenges as more useful services are added. offered by commerce become available.

IMPLICATIONS OF THE PROFESSIONALIZATION OF HACKERS:

Ultimately, the professionalization of the hacker industry means that anyone interested in tracking hackers must pay attention to anyone who is technically skilled enough to use these much more user-friendly tools (Level 3 [black hat/criminal] IoT hackers, and increasingly, non-technologists). This is because those interested in tracking hackers cannot afford to focus only on the technical innovators (Level 1 [script kiddies] and Level 2 [grey hat] IoT hackers). To put it another way, the professionalization of the hacker industry has made cyberattacks more accessible than ever. Nowadays, these people are mostly always non-state actors, yet anyone can hire these hacking platforms due to their widespread use and simplicity.

of usage, making them powerful potential weapons for state and non-state actors who want to act in a way that is either secret or implausible. The hacker business is become increasingly adaptable and adaptive as it gets more fully professionalized, making it more difficult for law enforcement and intelligence to combat. Hacking groups like China's APT31 (also called Zirconium)10 and Russia's Strontium (also called APT28 or Fancy Bear)9 still carry out malevolent assaults on Internet of Things devices. Hacking is and will continue to be dominated by skilled players who see themselves as "businessmen," much like other illegal businesses that have become professionalized, such as drug trading and human trafficking., Those who view law enforcement more as a regulatory force—that is, as an expense of doing business—than as a deterrent. When intelligence and law enforcement activities occur, these managers will swiftly reorganize their companies. The hacking industry will get more professionalized and change more quickly the more law enforcement forces it. Thus, the following are important queries for law enforcement and intelligence: How can the demands of law enforcement (such as constructing prosecutions) and intelligence-gathering (such as detecting and monitoring possibly harmful behaviors) be balanced? How can international law enforcement and intelligence collection activities against nonstate hackers be coordinated? The United States was able to do so in the early twentieth century.

- create a global alliance against drug trafficking; this might lead to the development of a unified front against hacking. Given that a dispersed solution to a distributed problem might really be the most successful strategy, how can we encourage citizen participation in indicting hacker activity?

HACKING AS A SERVICE: THE EVOLVING HACKER THREAT :

This paper's central thesis is that it is inaccurate to distinguish between the quickly growing field of cybercrime against the commercial sector and the direct threats posed by hacking to US national security, such as the theft of US government secrets, the disruption of vital infrastructure, or the penetration of military networks. Cyberespionage and cyberwarfare can be quickly conducted using the same methods and resources that are used to breach private systems for identity theft, fraud, or intellectual property theft [22]. The hacker industry's quick formalization, professionalization, and commercialization is creating networks and tools that are intended for deployment but are able to target states and governments in addition to firms or people [11]. As a result, the old analytical and jurisdictional divisions between cybercrime, cyberespionage, and cybersabotage are no longer valid.

According to Marcus Willet, a security expert, "Although the SolarWinds hack has been labelled a cyber 'attack', initial analysis indicates that it was intended not to damage, disrupt or destroy networks, but rather to gain intelligence." This assertion has drawn a lot of attention in relation to the offensive cyber, cyber security, and general national security strategies of the United States and its allies against these kinds of novel cyberattacks11. These new risks from the hacker business come at a huge cost as well. Financial institutions reported suspected ransomware payments totaling about $600 million, and US Treasury investigators have found billions more. Furthermore, the costs of identity theft to individuals and businesses are not included in this calculation.

In summary, both from an analytical and an interdiction standpoint, it is essential to approach the economic consequences of hacking and the national security risks of IoT hacking as a single, cohesive issue. In addition to exposing a more serious threat than is generally believed, examining the ways in which various hacking threat types interact offers analytical insight into how this cohesive threat is likely to develop. The professionalization of the hacker industry has made it crucial to take into account both the criminal and the traditional national security aspects of hacking as part of a strategy, even though law enforcement has historically been responsible for fighting cybercrime while the intelligence community and the Department of Defense (DoD) handled cyberwarfare and cyberespionage.

The hacker industry's growing array of goods and services, which aim to lower operational risks and boost business margins, has been a crucial component of its professionalization [11]. The hacker community today offers a different variety of exploits, tailors them to local and niche markets, and delivers them as "services" as well as products, in contrast to five years ago [11]. The hacker industry's innovation cycles seem to be quickening in the field of Internet of Things technologies. Potential hackers now face fewer technical obstacles to access because to hacker tools that are becoming more user-friendly and readily available online (such as Offensive Security's Kali LinuxPenetration Tool13). Hackers typically refrain from carrying out attacks personally in order to reduce personal risk, but instead

Participants in the hacker sector are no longer limited to Level 1, Level 2, or Level 3 hackers; in fact, some may not even be technologists due to the introduction of easy-to-use hacking tools that non-technical individuals can utilize. The evolution of hacker operations, teamwork, and management methods is thus significantly impacted by the involvement of non-technologists in the hacker business. An important analytical realization is that hackers' threat is no longer limited to Level 1, Level 2, and Level 3 operations carried out by technologists. Three hackers. This means that people with less technological expertise but a higher tolerance for legal risk are left to carry out the actual attacks. Here are a few of these: Although they do not perform the most economically significant labor, the technological innovators (Level 1 hackers) are the industry's pillars, just like in the real software sector. From the standpoint of the industry, Level 2 hackers who produce user-friendly rootkits, botnets, email lists, and other hacker industry main goods are equally as significant as Level 1 hackers who develop zero-day exploits. Similar to the real software business, the hacker community is made up of people with a wide range of specialized abilities who provide a number of unique services, such as marketing, engineers, salespeople, tech support, and so forth. Most of the time, non-techies will use the stolen identities, bank accounts, or credit cards to make purchases, take money out of bank accounts, and launder the money. Traditional criminal rather than technological hacking abilities are required for these downstream activities, which are essential to the hacker industry's operations.

A PRIMITIVE UNCERTAINTY:

Generally speaking, potential hackers can operate with more technological sophistication in areas with more Internet pipes. The ability to launch real-time attacks on systems and utilize unused bandwidth on compromised computers for more attacks is too alluring to pass up when broadband computers are permanently linked to the Internet. Because sophisticated hacking necessitates broadcasting and receiving massive amounts of data, substantial bandwidth is required. For instance, leveraging 5G to spread malware globally and recover stolen data from compromised machines demands a significant amount of capacity [12]. Consequently, high bandwidth is typically a prerequisite for the local development of a sophisticated hacker ecosystem and also presents an alluring target for outside hackers. As a result, the place where spam originates could not be the same as the region where the spammers reside. On the other hand, hackers are more likely to concentrate on low-bandwidth demanding exploits and, more importantly, social engineering attacks in low-bandwidth regions (such as Africa, North Korea, rural Asia, and Latin America) [12]. This overlap between professional, illegal hacking and government/military hacking is what makes hacking such a special difficulty. Professional hackers are mostly profit-driven businesspeople, but the governments that could seek to regulate them are, at bottom, profoundly ambivalent about halting hacking. Although all countries agree in principle that they would like to prohibit criminal hackers, many governments (including elements of the United States government) also have a desire to harness hacking talent and capabilities for offensive military reasons [46]. Because of this underlying ambiguity, it is more difficult for international governments to coordinate in order to stop hackers and secure computer systems than it is for attempts to combat international criminal organizations, like the world's drug trade. It is unclear whether governments view all hacking as harmful, even though in theory almost all of them concur that drugs are bad and are typically prepared to work with enemies to prevent their production and use. They simply consider it unethical to hack oneself (and perhaps their citizens). A choice to "go big" on either cybersecurity or offensive cyber-capabilities, as in that debate, not only suggests an assessment of the efficacy and likelihood of alternative threats and war modes, but it also radically changes the parameters (and possibly the possibility) of international cooperation to contain the threat. Since non-state actors are increasingly posing a threat to cyberspace, states' capacity to

CONCLUSION:

What will happen when more IoT devices are used by people throughout the world to connect to the internet? More than 27 billion IoT connections are expected to exist by 2025, according to IoT Analytics16. Although the demographics of this illegal economy are likely to change significantly, the hacker industry should be regarded as one of the great growth industries of the upcoming decade due to the rapidly declining barriers to entry for hacking and the possible lack of adequate economic opportunities available to the incoming generation of Internet users. Will organized crime play a bigger role in hacking? There is a lot of discussion among security specialists and law enforcement about the extent of mafia penetration of the hacker sector at the moment [5, 49, 23]. It is widely acknowledged that mafia-type organizations will probably certainly increase their involvement in cybercrime in the future17. Both the boundary between licit and criminal hacking activities and the line between online and offline illicit actions will become increasingly hazy. In other words, hacking may become just one division of a larger criminal organization as organized crime increasingly infiltrates the hacker industry. Thus, individuals who find strategic connections between their hacking and other endeavors will emerge victorious. It may become more difficult to distinguish between white hat security testing services and black hat extortion. The United States and other countries ultimately have to choose between law enforcement and the military/intelligence appropriation of hacking as a result of the professionalization of hacking. To comprehend the unforeseen repercussions of various types of international interdiction activities, future-focused analysis—including scenario planning—is crucial. A portion of the risk in this situation is iatrogenic, meaning that a large portion of the harm resulting from hacking may not originate from the actual hacking but rather from people's attempts to protect or shield themselves from it. In the event that ransomware assaults become more widespread, we might see the Internet become more fragmented and users retreat into separate "walled gardens." Unfortunately, this would not eliminate the threat posed by hackers, even if it would diminish the Internet's commercial and political importance as a communications platform that is open to all. To continue breaking into trustworthy online social networks, hackers would increase their use of social engineering, a technique that seems to be quite applicable in today's culture.

REFERENCES

[1] Abosata, Nasr, Saba Al-Rubaye, Gokhan Inalhan, and Christos Emmanouilidis. "Internet of things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications." Sensors 21, no. 11 (2021): 3654.

[2] Alexander, Bryce, and Adrian Baranchuk. "Cybersecurity and cardiac implantable electronic devices." Nature Reviews Cardiology 17, no. 6 (2020): 315-317.

[3] Alleyne, Brian, and A. J. Treviño. "Computer hacking as a social problem." The Cambridge Handbook of Social Problems 2 (2018): 127-42.

[4] Arief, Budi, and Denis Besnard. "Technical and human issues in computer-based systems security." School of Computing Science Technical Report Series (2003).

[5] Beebe, N. L., & Guynes, J. (2006). A model for predicting hacker behavior. AMCIS 2006 Proceedings, 409.

[6] Bizeul, David. "Russian business network study." unpublished paper, November 20 (2007).

[7] Bradley, Nicholas, Michelle Alvarez, John Kuhn, and David McMillen. "IBM 2015 cyber security intelligence index." IBM Security (2015).

[8] Burden, Kit, and Creole Palmer. "Internet crime: Cyber Crime—A new breed of criminal?." Computer Law & Security Review 19, no. 3 (2003): 222-227.

[9] Casino, Fran, Nikolaos Totosis, Theodoros Apostolopoulos, Nikolaos Lykousas, and Constantinos Patsakis. "Analysis and correlation of visual evidence in campaigns of malicious office documents." arXiv preprint arXiv:2103.16143 (2021).

[10] Chacko, Anil, and Thaier Hayajneh. "Security and privacy issues with IoT in healthcare." EAI Endorsed Transactions on Pervasive Health and Technology 4, no. 14 (2018).

[11] Chantzis, Fotios, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things. No Starch Press, 2021.

[12] Chettri, Lalit, and Rabindranath Bera. "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems." IEEE Internet of Things Journal 7, no. 1 (2019): 16-32.

[13] Choo, Kim-Kwang Raymond. "Money laundering risks of prepaid stored value cards." Trends and Issues in Crime and Criminal Justice 363 (2008): 1-6.

[14] Clark, David D., John Wroclawski, Karen R. Sollins, and Robert Braden. "Tussle in cyberspace: defining tomorrow's internet." In Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 347-356. 2002.

[15] Clarke, Richard A., Robert K. Knake, and Cyber War. "The Next Threat to National Security and What to Do About It New York: Ecco, 2010, ss. 290."

[16] Coleman, E. Gabriella, and Alex Golub. "Hacker practice: Moral genres and the cultural articulation of liberalism." Anthropological Theory 8, no. 3 (2008): 255-277.

[17] Coleman, E. Gabriella. "The social construction of freedom in free and open source software: Hackers, ethics, and the liberal tradition." (2005): 2270-2270.

[18] Cordesman, Anthony H., Justin G. Cordesman, and Justin G. Cordesman. Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland. Greenwood Publishing Group, 2002.

[19] Cybenko, George, Annarita Giani, and Paul Thompson. "Cognitive hacking: A battle for the mind." Computer 35, no. 8 (2002): 50-56.

[20] Davis, Robert WK, and Scott C. Hutchison. Computer crime in Canada: An introduction to technological crime and related legal issues. Carswell Legal Publications, 1997.

[21] Davidson, Ron. "The fight against malware as a service." Network Security 2021, no. 8 (2021): 7-11.

[22] Denning, Dorothy E. "Information Warfare and Security, Addsion-Wesley Longman." Inc., Reading, MA USA (1999).

[23] Djenna, Amir, and Diamel Eddine Saïdouni. "Cyber attacks classification in IoT-based-healthcare infrastructure." In 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1-4. IEEE, 2018.

[24] Ellis, Ryan, and Yuan Stevens. "Bounty Everything: Hackers and the Making of the Global Bug Marketplace." Available at SSRN 4009275 (2022).

[25] Farsole, Ajinkya A., Amurta G. Kashikar, and Apurva Zunzunwala. "Ethical hacking." International Journal of Computer Applications 1, no. 10 (2010): 14-20.

[26] Flickenger, Rob. Wireless hacks. " O'Reilly Media, Inc.", 2003.

[27] Giani, Annarita. "Detection of attacks on cognitive channels." PhD diss., Dartmouth College, 2006

[28] Hafner, Katie, and John Markoff. Cyberpunk: outlaws and hackers on the computer frontier, revised. Simon and Schuster, 1995.

[29] Hartmann, Björn, Scott Doorley, and Scott R. Klemmer. "Hacking, mashing, gluing: a study of opportunistic design and development." Pervasive Computing 7, no. 3 (2006): 46-54.

[30] Hoath, Peter, and Tom Mulhall. "Hacking: Motivation and deterrence, part I." Computer Fraud & Security 1998, no. 4 (1998): 16-19.

[31] Hollinger, Richard C. "Evidence that Computer Crime Follows a Guttman-Like Progression." Sociology and Social Research 72, no. 3 (1988): 199-200.

[32] Holt, Thomas J. Hacks, cracks, and crime: An examination of the subculture and social organization of computer hackers. University of Missouri-Saint Louis, 2005.

[33] Kagita, Mohan Krishna, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Saurabh Singh. "A review on cyber crimes on the Internet of Things." In Deep Learning for Security and Privacy Preservation in IoT, pp. 83-98. Springer, Singapore, 2021.

[34] Kramp, Thorsten, Rob van Kranenburg, and Sebastian Lange. "Introduction to the Internet of Things." In Enabling Things to Talk, pp. 1-10. Springer, Berlin, Heidelberg, 2013.

[35] Lambet, Paul. "Equifax Data Breach, 143 Million Only Tip of the Iceberg." Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns. 1 (2017): 30. [36] Lee, J. C. "Hacking the Nintendo Wii Remote. 2008." IEEE Pervasive Computing 7, no. 3 (2012).

[37] Leeson, Peter T., and Christopher J. Coyne. "The economics of computer hacking." JL Econ. & Pol'y 1 (2005): 511.

[38] Levy, Steven. Hackers: Heroes of the computer revolution. Vol. 14. Garden City, NY: Anchor Press/Doubleday, 1984.

[39] Luiijf, Eric. "Understanding cyber threats and vulnerabilities." Critical infrastructure protection (2012): 52-67.

[40] Liu, Simon, and Bruce Cheng. "Cyberattacks: Why, what, who, and how." IT professional 11, no. 3 (2009): 14-21.

[41] Jahankhani, Hamid, and Ameer Al-Nemrat. "Global e-security." In International Conference on Global e-Security, pp. 3-9. Springer, Berlin, Heidelberg, 2008.

[42] Jasanoff, S. "A sociology of Hackers." The Sociological Review 46, no. 4 (1998): 757-780.

[43] Joffee, Rodney. "Cybercrime: the global epidemic at your network door." Network security 2010, no. 7 (2010): 4-7.

[44] Matyus, Allison. "Facebook faces another huge data leak affecting 267 million users." Digital Trends 19 (2019).

[45] Margolis, Joel, Tae Tom Oh, Suyash Jadhav, Young Ho Kim, and JeongNeyo Kim. "An in-depth analysis of the mirai botnet." In 2017 International Conference on Software Security and Assurance (ICSSA), pp. 6-12. IEEE, 2017.

[46] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

[47] Milone, Mark. "Hacktivism: Securing the national infrastructure." Knowledge, Technology & Policy 16, no. 1 (2003): 75-103.

[48] Mohurle, Savita, and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017." International Journal of Advanced Research in Computer Science 8, no. 5 (2017): 1938-1940.

[49] Mugweni, Benison, and Rose Mugweni. "New Patterns in Cyber Crime with the Confluence of IoT and Machine Learning." In ICT and Data Sciences, pp. 117-133. CRC Press, 2022.