Borneo International Journal eISSN 2636-9826; Vol. 6 (3); 2023; 1-6
Published by *Majmuah Enterprise*
www.majmuah.com

An Analysis of Future Strategies to Protect Against Hackers

MOHD HAFIZ ALI MOHD ANUAR and MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email: hafiz_ali@usm.my , m.fadli.zolkipli@uum.edu.my | Tel: +60125318364 , +60177247779 |

Received: July 12, 2023
Accepted: July 24, 2023
Online Published: Sept 01, 2023

Abstract

In these articles, we take a deep dive into the ever-changing nature of hacking, its effects on cybersecurity, and future strategies to combat it. The difficulty of ensuring cyber security is further heightened by the fact that the study shows how technology, policy, and human factors all interact with one another. We look at how modern hacking techniques including phishing attacks, malware, exploiting outdated software, password cracking, and Denial of Service (DoS) may have far-reaching effects. Future hacking is expected to be characterized by a rise in AI-driven attacks, Internet of Things vulnerabilities, sophisticated ransomware, state-sponsored cyber-attacks, and cloud vulnerabilities. We propose a three-pronged strategy for addressing these threats: technological remedies; robust regulation and governance; and an increased emphasis on human factors and awareness. The paper highlights the need for a flexible, multi-layered security system capable of adapting to the ever-evolving character of cyber threats. The study promotes a sophisticated knowledge of cybersecurity and offers a road map for future resistance against hackers by combining the latest academic research with long-term strategic planning.

Keywords: Hacking, Cybersecurity Strategies, Future Cyber Threats, Evolution of Hacking, Countermeasures Against Hacking

1. Introduction

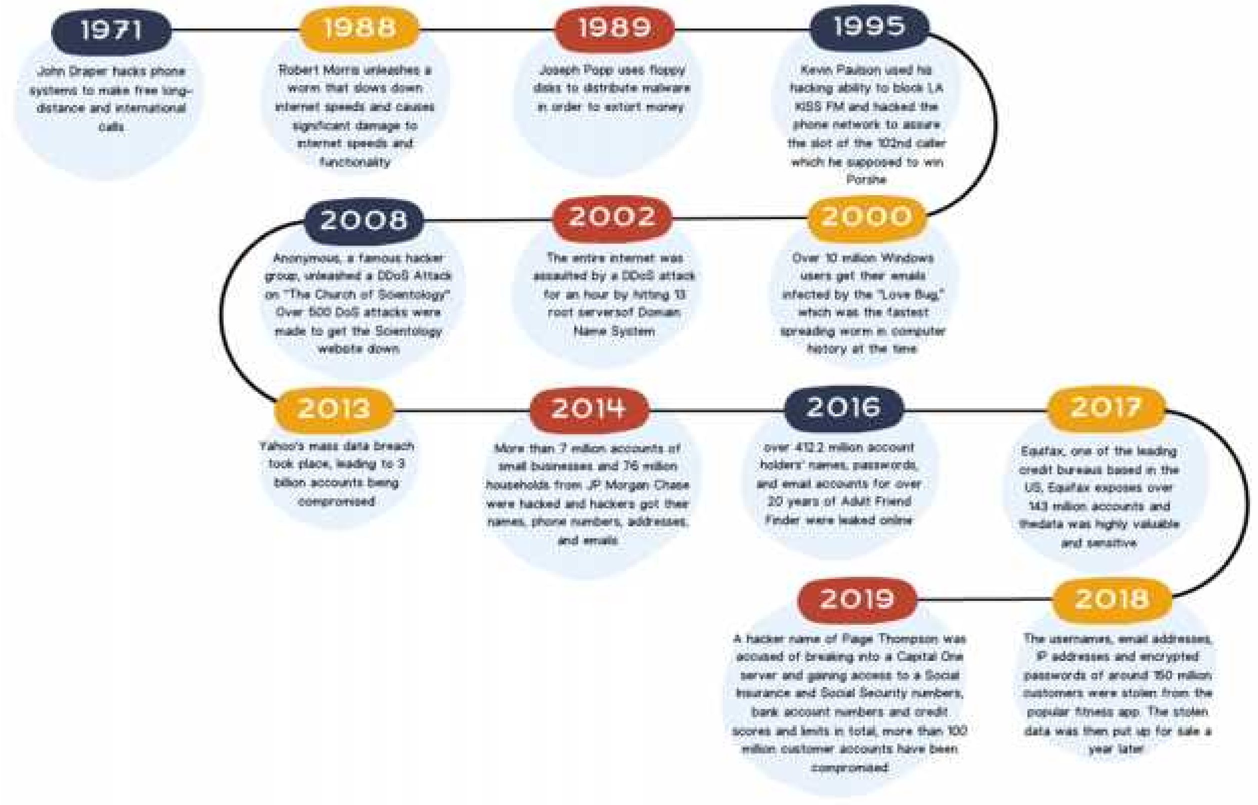
Safety and security in our digital settings are of fundamental importance in today's increasingly digital society. Constant technological progress makes us vulnerable to a wide variety of cyber hazards, most of which come from people or organizations often referred to as "hackers" who take advantage of these openings and pose serious risks to our online safety. Our investigation, grounded in the nuances of the online world, sheds light on a variety of hacking methods, from sneaky phishing to full-out DoS assaults. These methods pose serious threats to both persons and organizations, since they may result in theft of sensitive data, disruption of operations, and substantial financial losses. In addition to studying present cyberthreats, our research is focused on foreseeing and comprehending those that may emerge in the future. The trajectory of cyber threats, which is increasing in complexity, targeted accuracy, and potential disruptiveness, may be better predicted with this kind of forward-thinking strategy. Our analysis culminates in actionable solutions to counter these dangers. These include various responses, from legislation shifts and technological improvements to public awareness campaigns and classroom instruction. The goal of these preventative actions is to provide people and businesses with a flexible method of coping with the ever-changing cyber threat scenario. The findings of this research hope to improve the knowledge of cybersecurity, allowing for more thorough preparation for potential attacks.

2. Overview of Hacking

Hacking is the capable use of systems, usually computer systems, to do things that were not meant to be done with them. Even though the word "hacking" does not necessarily mean that someone is trying to do something bad, it is often used to describe illegal actions, especially cybercrime. Hackers have come to be individuals who use these methods with bad intentions, taking advantage of digital vulnerabilities to make money or cause trouble. Hacking has been around since the middle of the 20th century (Jordan, 2017), but it became much more dangerous when the digital age began. As technology became increasingly prevalent in our lives, it also became easier for bad people to use digital flaws to do terrible things. When the first malicious computer worms and high-profile data breaches happened (Mohammed. I. Alghamdi, 2021), it was the start of a time when cyber threats got worse, and hacking became a major global worry again.

3. History of Hacking

There have been an infinite number of cyberattacks throughout the chronicles of digital history, each with its own scope, severity, and level of complexity. The incidents represent major milestones in the field of cybersecurity and have contributed invaluable knowledge to our comprehension of the ever-changing threat landscape. These significant cyber-attacks, ranging from data breaches affecting millions of end-users to orchestrated, state-backed cyber offensives targeting vital infrastructures, have highlighted the inherent vulnerabilities of our hyperconnected world and the critical need for comprehensive cybersecurity mechanisms. In evaluating these occurrences through a retrospective lens, we continually obtain new insights and modify our protective strategies to prevent future threats. While this summary in Figure 1 provides a glimpse of the vast spectrum of cyberattacks that have occurred, it fundamentally emphasizes the necessity of developing and implementing robust, effective, and adaptive cybersecurity strategies in our collective pursuit of digital security and resilience.



1971
John Draper hacks phone systems to make free long-distance and international calls

1988
Robert Morris unleashes a worm that slows down internet speeds and causes significant damage to internet speeds and functionality

1989
Joseph Popp uses floppy disks to distribute malware in order to extort money

1995
Kevin Paulson used his hacking ability to block LA KISS FM and hacked the phone network to assure the slot of the 102nd caller which he supposed to win Porshe

2000
Over 10 million Windows users get their emails infected by the "Love Bug," which was the fastest spreading worm in computer history at the time

2002
The entire internet was assaulted by a DDoS attack for an hour by hitting 13 root serversof Domain Name System

2008
Anonymous, a famous hacker group, unleashed a DDoS Attack on "The Church of Scientology" Over 500 DoS attacks were made to get the Scientology website down

2013
Yahoo's mass data breach took place, leading to 3 billion accounts being compromised

2014
More than 7 million accounts of small businesses and 76 million households from JP Morgan Chase were hacked and hackers got their names, phone numbers, addresses, and emails

2016
over 412.2 million account holders' names, passwords, and email accounts for over 20 years of Adult Friend Finder were leaked online

2017
Equifax, one of the leading credit bureaus based in the US, Equifax exposes over 143 million accounts and thedata was highly valuable and sensitive

2018
The usernames, email addresses, IP addresses and encrypted passwords of around 150 million customers were stolen from the popular fitness app. The stolen data was then put up for sale a year later

2019
A hacker name of Paige Thompson was accused of breaking into a Capital One server and gaining access to a Social Insurance and Social Security numbers, bank account numbers and credit scores and limits in total, more than 100 million customer accounts have been compromised

Figure 1: Hacking Events and History in 50 years (Sources: (Catherine Hiley, 2022; Mohammed. I. Alghamdi, 2021))

According to (Mohammed. I. Alghamdi, 2021) and (Catherine Hiley, 2022) the history of hacking shows a clear change in the level of technological sophistication, the reasons for hacking, and the effects on society. Early cases of hacking, like the break-in to ARPANET in 1971, were often the result of curious people trying out new digital systems. Most of these things were done to push the limits of what was possible technologically, without the bad intentions that are typical of many hacking operations today. As the digital age came about at the end of the 20th century, hacking went from being a niche activity to a business with a lot of promises to change things. This was shown by the wide spread of malware like the Morris Worm, which was one of the first worm viruses to be spread over the Internet in 1988. This was a turning point toward more harmful cyber actions meant to affect many people. Cyberattacks increased in frequency and severity as the new millennium began, and massive data breaches became the norm. The Yahoo data breach in 2014 was a good example. It showed that even big companies are vulnerable to savvy cyber threats and that there is a lot of money to be made by taking advantage of software flaws. With the rise of state-sponsored strikes, cybersecurity has become a more critical issue on the international stage in recent years. The actions of groups like the Equation Group and Advanced Persistent Threats (APTs) show that cyberattacks could be used as tools of state policy. This gives cybersecurity an important geopolitical dimension.

From its simple beginnings to its complex and geopolitically important state today, hacking shows how cybersecurity dangers are always changing. This historical trend shows how important it is to keep improving cybersecurity means to keep up with the growing and changing threat landscape. Hacking and the dangers it brings have changed a lot over time, and so have the ways to protect against these risks. Initial security measures focused on setting up a "perimeter defense," which is like a castle and meant to keep people out. But as threats got more complicated and businesses became more connected, it became clear that a more comprehensive, multi-layered method was needed. Today's defensive plans recognize the limits of the "perimeter defense" and focus on the idea of "defense in depth." This method calls for multiple layers of defense at various levels, including technological solutions, policy measures, and security knowledge among people. In this paper, we look at how these countermeasures are changing to keep up with the changing nature of hacking. This adds to our larger talk about how to protect against hackers in the future.

4. Understanding About Hacking

Table 1 offers an insightful overview of predominant hacking methods, the measures currently employed to counteract them, and the impacts these methods have on cybersecurity **(Hussain, Mohamed, & Razali, 2020)**.

	Hacking Method	**Current Countermeasures**	**Impact on Cybersecurity**
1	Social Engineering & Phishing	Security awareness training, anti-phishing tools	Unauthorized access, data breaches
2	Malware	Anti-malware software, regular software updates	Data theft, system disruption
3	Missing Security Patches	Regular system updates, vulnerability management	System vulnerabilities, unauthorized access
4	Password Cracking	Strong password policies, multi-factor authentication	Unauthorized access, data breaches
5	DDoS	Firewalls, load balancing, network redundancy	Service disruption, financial loss

Table 1: Comparison of Hacking Methods and Countermeasures

Starting with "Social Engineering and Phishing," these methods often use fake emails that look like they came from trusted sources. A common phishing plan is an email that looks like it came from a bank and asks the user to update their account information. Current defenses include security training that teaches people how important it is to check the source of emails and anti-phishing tools that can find and block phishing efforts. (Hatfield, 2018) Malware is a broad term that includes many diverse types of bad software, like Trojans, blackmail, and spyware. One famous example is the WannaCry virus, which locked up files on the victim's computer and asked for money to unlock them. The best way to protect against these dangers is with anti-malware software like Norton or McAfee and regular software updates. **(Martens, Wolf, & Marez, 2019)**

"Missing Security Patches" create holes that can be used to get into systems without permission. For example, the WannaCry virus took advantage of known weaknesses in the Microsoft Windows operating system. Such risks can be reduced with the help of regular system changes and strong vulnerability management systems like Nessus. In the "Password Cracking" category, brute force attacks are included. In these attacks, a hacker carefully tries all password combinations until the right one is found. Tools like LastPass or 1Password that encourage strong password rules and multi-factor authentication (like biometric or OTP verification) can help stop these threats. **(Bhana & Flowerday, 2020)** Lastly, overloading a network with too many requests is the hallmark of a "DDoS" attack. The Dyn cyberattack in 2016 is a widely recognized example since the attack brought down major websites such as Twitter, Netflix, and Reddit. Firewalls, load balancing, and redundant networks are all effective strategies to combat these threats. **(Rathore & Vaish, 2020)** In the end, these diverse ways to hack require different, custom-made solutions. As the conversation goes on, we will talk more about how to make stronger defenses against these and other hacking ways in the future.

5. Future Trend in Hacking

Anticipating future trends in hacking requires understanding both the technological advancements and the socio-economic factors that drive changes in the cyber threat landscape. Some future possibilities are listed here.:

- Artificial Intelligence and Machine Learning: The evolving of this (Sarker, 2021), hackers may leverage these technologies to automate and streamline their attacks. For instance, we could witness highly targeted phishing emails designed by AI systems that have been trained on vast amounts of personal data, making the deceptive emails almost indistinguishable from legitimate ones. Similarly, we might see the rise of intelligent malware that can adapt its behavior to evade detection by learning from the defense mechanisms it encounters.

- Internet of Things (IoT) Vulnerabilities: As the IoT continues to grow, with more devices connecting to the internet, the scale of potential attacks could increase dramatically. For example, hackers could develop advanced botnets that harness the power of millions of compromised IoT devices to launch devastating DDoS attacks. In a worst-case scenario, critical infrastructure linked to IoT devices, such as power grids or healthcare systems, could be disrupted.

- Ransomware Evolution: In the future, we might see ransomware attacks evolving to become more destructive and disruptive (Mohammed. I. Alghamdi, 2021). Attackers could use more complex encryption algorithms, making decryption impossible without the specific key. Additionally, they might develop ransomware that targets cloud-based backup systems, thus nullifying one of the key defenses against ransomware attacks **(Kanter GP, Kufahl J, & Cohen IG, 2021)**.

- State-Sponsored Cyber Attacks: The sophistication and complexity of these assaults is only anticipated to rise. Deep fakes, whereby plausible but false movies or audio recordings are produced to propagate misinformation or sway public opinion, may be used in future assaults. In addition, key infrastructure might be attacked by state-sponsored hackers, leading to widespread disruption and fatalities. (Shackelford et al., 2017).

- Cloud Vulnerabilities: As more data and services move to the cloud, we might see an increase in "cloud hopping" attacks **(Barrowclough & Asif, 2018)**. In this scenario, hackers compromise one cloud user and then use that to gain access to other users on the same multi-tenant cloud server. Furthermore, as companies increasingly rely on third-party cloud services, the risk of supply chain attacks also increases (Yeboah-Ofori et al., 2021).

In conclusion, the landscape of cyber threats is becoming more complex and potentially damaging. This highlights the urgent need for comprehensive, forward-looking cybersecurity strategies to mitigate the potential impact of these emerging threats.

6. Future Strategies to Protect from Hackers

When designing protection strategies, it is important to consider both the present and anticipated trends in hacking. Protection plans should include a mix of technical solutions, policy enforcement, and user education. Considering the many ways now used for hacking, below are some strategies:

Technological Measures:

- Enhanced Authentication: When it comes to online banking, clients are frequently required by financial institutions to utilize two-factor authentication (2FA). In most cases, the user will be required to enter a password in addition to a one-time PIN that will be issued to their mobile device **(Oppliger, Hauser, & Basin, 2006)**.

- Network Monitoring and Anomaly Detection: Darktrace, a business that specializes in network security, employs artificial intelligence to monitor networks and detect and respond to cyber-attacks in real time (Krishnappa, 2023). The system can recognize anomalous data patterns and behaviors that depart from the norm, which may indicate malevolent intent.

- Proactive Defense Measure: Intrusion prevention systems and firewalls are two examples of proactive defense measures that are used by Cisco's Talos (Cisco Security Threat Intelligence Organization, 2019), which is a threat intelligence group. These are used to proactively identify threats and safeguard network infrastructures.

- Secure IoT Devices: Apple's HomeKit architecture for smart home gadgets calls for severe security measures to be implemented, including end-to-end encryption and secure chipsets in all devices **(Haque & Tasmin, 2020)**.

- Data Backups and Encryption: Many companies rely on cloud services for their regular data backups **(Ryz & Grest, 2016)**, such as Amazon's AWS Backup, and employ Amazon Web Services' Key Management Service for their data encryption needs.

- Secure Cloud Configurations: Enterprises like Dome9 offer services for continuously ensuring cloud security and compliance. These services assist enterprises in enforcing appropriate security policies within their cloud environments **(Barrowclough & Asif, 2018)**.

Policies and Governance Measures:

- Robust Patch Management: Microsoft fixes any known vulnerabilities that could be exploited by cyber attackers by providing regular patches to its software products (such the Windows OS). These patches can be downloaded from the company's website **(Kanter, Kufahl, & Cohen, 2021)**.

- Incident Response Plans: As a direct result of the WannaCry assault in 2017, the National Health Service (NHS) in the United Kingdom developed a comprehensive incident response plan to lessen the damage caused by future attacks of a similar nature.

- Adherence to Prescribed Safety Measures To protect their customers' credit card information, businesses that process credit card transactions must adhere to the Payment Card Industry Data Security Standard (PCI, 2009).

Human Factors and Awareness:

- Security Awareness Training: Google has an in-house training program called "Phishing Expedition" that teaches employees how to spot and respond appropriately to phishing attempts **(Jung, Choi, & Park, 2022)**.

- Culture of Security: IBM has cultivated a culture of security in which each employee is regarded as a "human firewall" and is encouraged to play an active role in the company's efforts to thwart cyberattacks. This culture of security has led to the company's success in thwarting cyberattacks **(Chng, Lu, Kumar, & Yau, 2022)**.

The significance of anticipating and preparing for future cybersecurity challenges cannot be overstated as technological innovation continues. By proactively adopting these countermeasures, we can secure our digital future and remain one step ahead of hackers.

7. Conclusions

In conclusion, the constant evolution of cybersecurity demonstrates the need for robust, adaptable strategies that can address both current and future threats. Our examination of common hacking techniques, such as social engineering and phishing, malware, exploiting missing security updates, password cracking, and DDoS attacks, demonstrates the complexity and diversity of modern cyber threats. Their effects on cybersecurity, such as data disclosures and service interruptions, demonstrate how dangerous they are to individuals, businesses, and nations. The future trend of hacking, which will be characterized by the combination of AI and ML, the rise of Internet of Things (IoT) vulnerabilities, the development of ransomware, the rise of state-sponsored cyber-attacks, and the vulnerability of cloud services, poses a significant threat to cybersecurity. Notably, each of these trends is likely to make cybersecurity even more complicated, necessitating more sophisticated and adaptable defensive strategies.

To effectively counter these threats, an integrated plan incorporating technology, policy and governance, and human factors and awareness is required. The first line of defense against cyber threats consists of technological measures such as improved authentication, network monitoring, the detection of anomalies, and proactive defense measures. In addition, effective cybersecurity governance is founded on robust patch management, incident response plans, and adherence to security standards. Lastly, it is essential to cultivate a security-aware perspective, as people are frequently one of the greatest vulnerabilities in cybersecurity. As cyber threats become more complex and deadly, our defenses must evolve and adapt. Due to this, we must invest in the research and development of sophisticated cybersecurity technologies, robust governance policies, and comprehensive training. This integrated approach, which is based on a thorough understanding of both current and future threats, is our greatest defense against the growing cybersecurity challenge in the digital age.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Barrowclough, J. P., & Asif, R. (2018). Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures. *Security and Communication Networks*, 2018. Retrieved from https://doi.org/10.1155/2018/1681908

Bhana, B., & Flowerday, S. (2020). Passphrase and keystroke dynamics authentication: Usable security. *Comput. Secur.*, 96, 101925.

Catherine Hiley. (2022). Brief history of cybersecurity and hacking. Retrieved 9 July 2023, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, 5, 100167. Retrieved from https://doi.org/https://doi.org/10.1016/j.chbr.2022.100167

Cisco Security Threat Intelligence Organization. (2019). Talos Intelligence .

Haque, A. K. M. B., & Tasmin, S. (2020). Security Threats and Research Challenges of IoT - A Review. *Journal of Engineering Advancements*, 01(04), 170–182. Retrieved from https://doi.org/10.38032/jea.2020.04.008

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Comput. Secur.*, 73, 102–113.

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*. New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3386723.3387847

Jordan, T. (2017). A genealogy of hacking. *Convergence*, 23(5), 528–544. Retrieved from https://doi.org/10.1177/1354856516640710

Jung, Y., Choi, E., & Park, N. (2022). Educational Aids for Teaching Hacking Principles to Strengthen Computational Thinking Skills to Elementary. *Webology*.

Kanter, G. P., Kufahl, J., & Cohen, I. G. (2021). Beyond Security Patches—Fundamental Incentive Problems in Health Care Cybersecurity. *JAMA Health Forum*, 2(10), e212969–e212969. Retrieved from https://doi.org/10.1001/jamahealthforum.2021.2969

Kanter GP, Kufahl J, & Cohen IG. (2021). Beyond Security Patches—Fundamental Incentive Problems in Health Care Cybersecurity. In *JAMA Health Forum*.

Krishnappa, T. (2023). *A REVIEW ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN PREVENTING CYBER THREATS*. *International Journal of Engineering Applied Sciences and Technology* (Vol. 8). Retrieved from http://www.ijeast.com

Martens, M., Wolf, R. De, & Marez, L. De. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Comput. Hum. Behav.*, 92, 139–150.

Mohammed. I. Alghamdi. (2021). History, Present 2021 and Future of Cyber Attacks. *Journal of Journal of Cybersecurity and Information Management*, 8(2), 71–83.

Oppliger, R., Hauser, R. C., & Basin, D. A. (2006). SSL/TLS session-aware user authentication - Or how to effectively thwart the man-in-the-middle. *Comput. Commun.*, 29, 2238–2246.

PCI, S. S. C. (2009). *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*. Retrieved from www.pcisecuritystandards.org.

Rathore, M., & Vaish, A. (2020). A system design for multi-phase, hybrid DDoS detection. *Computer Fraud & Security*, 2020(11), 10–19. Retrieved from https://doi.org/https://doi.org/10.1016/S1361-3723(20)30119-6

Ryz, L., & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security*, 2016(3), 18–20. Retrieved from https://doi.org/https://doi.org/10.1016/S1361-3723(16)30028-8

Sarker, I. H. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. Retrieved from https://doi.org/10.20944/preprints202101.0457.v1

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Deckard, A., … Smith, J. (2017). Making Democracy Harder to Hack. *University of Michigan Journal of Law Reform*, (50.3), 629. Retrieved from https://doi.org/10.36646/mjlr.50.3.making

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, 9, 94318–94337. Retrieved from https://doi.org/10.1109/ACCESS.2021.3087109