Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 1 – 7 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

SYSTEM SURVIVABILITY THREATS AND FACTORS INFLUENCING ATTACKS IN HEALTH FACILITIES

Joseph SIMIYU[1] Dorothy RAMBIM[1], Jasper ONDULO[1]

[1]Masinde Muliro University of Science and Technology, 190, Kakamega, 50100, Kenya

ABSTRACT: The adoption of e-health offers affluence medical benefits, unfortunately source of effective data is poorly protected, it is also susceptible to dangerous threats and attacks. While the volume of medical data dictates the use of technology, a failure of e-health systems to include security survivability as apriority in making e-health systems compromise easier. With this numerous security issues, the system can suffer more and never recover to assure users on their mission mandate. Despite efforts to secure Kenya's cyber space by assuring Kenya electronic transactions and online services such as e Government and health, system survivability and security attacks continues to jeopardize e-health confidentiality, credibility, reliability and availability for both providers and users. Therefore, it is important to understand issues around system survivability after attack rather than just security. Overall, this paper will try to come up with a system survivability issues for fighting information systems crime in the health sector in Kenya. Specifically, this research study will seek to outline the major system survivability threats and vulnerabilities within health sector in Kenya.

KEYWORDS: e-health, Survivability, System Vulnerabilities, Security Risks

1. INTRODUCTION

Survivability is defined as the ability of a system to provide essential services in the presence of attacks and failures, and to recover full services in a timely Manner. According to M. Farrukh Khan, Raymond A. Paul, in Advances in Computers, 2012) [i]. Survivability has been considered as a key inherent property of a reliable system. A survivable system continues to function, despite the presence of malicious attacks or arbitrary faults. The fact that a system has well-defined functions and correct implementations does not guarantee that the system is survivable. Some damages, which are resulted from novel, well-orchestrated malicious attacks, are simply beyond the abilities of most system developers to predict. In those situations, even a strong system with well-established security could possibly be compromised.

Globally Information technology is a very important tool in any current organization. Today organizations are driven by emerging technologies of which when implemented improve the welfare of clients and changes how people interact and promote social participation. These new technologies improve the productivity and competitiveness of organizations while opening up new areas to be explored and creating business and job opportunities as hold forth by Shenoy, A., & Appel, J. M. (2017).[ii].

In Africa, many countries have reported the upsurge of digital threats and malicious activities. The threats has been as a results of sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups. While the individual governments on the continent seem to be very slow to appreciate the importance of the concept of information systems safety, the regional political body, the African Union (AU) seems to be making some gains in raising awareness and advocating for better cyber safety, to the continent's ministers of Information and Communications Technology. The African Union Commission (AUC) put out a call for experts to join its African Union Cyber Security Expert Group (AUCSEG) based on a resolution by its executive council and also created Africa Cyber Security collaboration and coordination committee to advise the AUC and policy makers on Cyber strategies, with many other specific tasks. Call for experts, AU, (2018)[iii]

This study determines the nature and characteristics of threats, assess the emerging threats and vulnerabilities that influence the health sector in Kenya and more specifically Referral Hospital hospitals. A qualitative review was undertaken by a literature search of the survivability and vulnerabilities to identify threats and the factors influencing system survivability attacks in healthcare.

In this paper, we examine the major system survivability threats and factors influencing them in healthcare facilities. The rest of the paper is organized as follows, II. provides emerging survivability threats and vulnerabilities in the health facilities, Factors Influencing system survivability attacks in healthcare is provided in section III, section IV discussion and conclusion.

2. EMERGING SYSTEM SURVIVABILITY THREATS AND VULNERABILITIES IN THE HEALTH FACILITIES

There are several issues that make health care security more complicated and have increased vulnerability over time (Burns, 2016)[iv]. In addition to this proliferation in emerging technology, many healthcare companies tend to use obsolete systems in many fields, such as Window XP, which has not been supported since 2014. (Milliman, 2016)[v], enabling hackers and malware to easily avoid detection, for example, the recent WannaCry attack. The propriety nature of medical device software means that healthcare IT teams may not be able to access the internal software in medical devices, so they rely on manufacturers to build and maintain security in those devices which were lacking. There is also a problem with lack of funding for security and system survivability, while hospitals and other organizations spend funding to become more integrated; they do not spend enough time and money to keep software updated and systems safe (Kotz *et al*., 2016)[vi]. This is exacerbated by a lack of industry expertise on system survivability security resulting from a general lack of technology and the prohibitive expense of security personnel. In summary, a rapid shift to electronic health records and interconnected devices, along with historical and ongoing lack of investment in survivability of systems and a lack of understanding of health personnel's safety work behaviors have made the health sector vulnerable to attacks.

Although healthcare has vulnerabilities to exploit, attackers need to be motivated to commit attacks. Motivation includes the potential for financial and political benefit and possibly taking life in a cyberwarfare process. Economic benefit is the highest of those motivations. Data on health care is far more valuable than any other data. The value can exceed €888.05 for a complete set of medical credentials (Sulleyman, 2017). Stolen medical identification may be used by claiming somebody's identity or insurance records to access health care and prescription drugs. Uses extend to organized crime perpetrating sophisticated fraud. Fraudsters have earned billions in the last few years by filing fraudulent claims and dispensing drugs to sell on the dark web (McCarthy, 2016). Sometimes there is even sufficient information in medical records to open bank accounts, secure loans or obtain passports.

Effects of Cybercrime on Healthcare: The health sector has seen a drastic increase in the amount and scale of data breaches in the last few years. Breaches lead to financial loss, reputational loss and reduced patient safety. Report indicates the average cost of missing or stolen medical records containing confidential and sensitive information is massive (Seh AH, 2020)[vii], and continued advertisement associated with large breaches may jeopardize patient trust which may result in less willingness to share data (Whitler, 2017**)**[viii]. This is especially problematic for patients with conditions such as sexual or mental health conditions being stigmatized.

Despite warnings issued and the availability of security patches, the scale of the WannaCry attack was exceptional, with over 300,000 computers worldwide demanding that users pay ransoms on bitcoin (Scott & Wingfield, 2017)[ix]. A number of hospitals have experienced system wide lockouts, patient care delays, and loss of function in connected devices such as MRI scanners, and refrigerators for blood storage. This attack was not directed specifically at healthcare organizations, yet the damage was widespread. Other ransomware targeted specifically the healthcare sector.

Many malware attacks have led to major incidents, such as healthcare trust suffering an unspecified cyber-attack which results in the shutdown of IT systems and scheduled operations and outpatient appointments being cancelled for days (Evenstad, 2016)[x]. Medjack (Medical Device Hijack) is attack that was detected to inject malware into unprotected medical devices for lateral movement through the hospital network (Storm, 2015)[xi]. The infected medical devices creates poor ties in hospital safety defenses, including diagnostic equipment (including MRI machines), therapeutic equipment (e.g., infusion pumps), and life-supply equipment (including ventilators).

Simulated attacks by 'White Hacker' have highlighted that there are other vulnerabilities which mean "Medical devices are the next security nightmare". There is potential for attacks similar to what used to be considered science fiction. For example, brain jacking where a suitable device could be inserted (Pycroft *et al*., 2016)[xii]. Simulated attacks on devices such as pacemakers and defibrillators, insulin pumps and pumps for drug infusion have been carried out. These attacks have remotely controlled machines to modify surgery or send lethal doses of drugs. Though currently only simulated such attacks may occur (Klonoff, 2015)[xiii]. Risks will continue to increase if cybersecurity has not been designed from the start of the product or project lifecycle.

Ransomware and other Malware: Malware is a serious problem across all industries, however, in healthcare, a malware infection can mean life or death. Healthcare operates an intricate series of interconnected reporting and services. The interlocking network that communicates information on our behalf to better our health is especially vulnerable to ransomware and other malware attacks. In the aforementioned NHS WannaCry attack, hospitals are forced to close their doors to new patients, and existing patients' treatment are interrupted because of an inability to access records. The HHS 'Wall of Shame', which lists healthcare data breaches data breaches affecting almost millions of individuals. Healthcare is among the leading cyber-criminal-targeted industries (Kruse et al., 2017)[xiv]. Breaches may be caused by hacking, malware and threats to insiders. While insider threats are issues created by employee errors or deliberate actions (e.g., responding to phishing emails, a social engineering attack to extract login credentials or launch a malware attack, erroneous security settings, password misuse, loss of laptops and sending unencrypted emails). This thus becomes a moderating factor together with DDOS and ransomware attacks.

Ransomware exploits vulnerabilities to hijack monetary benefit infrastructures for target information technology (IT). Because of the nature and value of information, access to medical information allows cyber criminals to commit identity theft, medical fraud, and extortion, and to illegally get controlled substances. Medical information's utility and versatility, extensive centralized storage of medical information, relatively weak IT security systems, and the expanding use of healthcare IT infrastructure all contribute to an increase in cyber-attacks on healthcare institutions. Research suggests that an individual's medical information is 20–50 times more valuable to cyber-criminals than personal financial information (Kruse *et al*., 2017). As such, cyber-attacks targeting medical information are increasing 22% per year (Kruse *et al*., 2017). Ransomware uses a hybrid encryption system that combines the two cryptographies to create an asymmetric cryptosystem in which data is encrypted using a randomly generated symmetric key, which is then encrypted using a public key where one party has the appropriate private key (Krisby, 2018)[xv]. The cyber-criminal uses the private key to decrypt the symmetric key to decrypt the data back "into "plaintext" and give the key back to the victim, who can then use it to access their device again (Krisby, 2018). When encrypted, the code is unavailable and indecipherable. The user receives a pop-up notification that requires a ransom payment (usually in untraceable digital currency such as bitcoin) in exchange for the decryption key (Pope, 2016)[xvi].

Often, Ransomware does not destroy data but will lock up data before a ransom is paid (Richardson & North, 2017)[xvii]. Even if the infection with ransomware is removed the data can remain encrypted. But it is necessary to remember that the mere infection of a ransomware computer does not suffice. To get an encryption key and report its results, the ransomware has to communicate with a server (Richardson & North, 2017). This includes a server hosted by a corporation that avoids criminal activity and ensures anonymity for the attackers (called Bulletproof Hosting). These businesses are often located in China or in Russia (Richardson & North, 2017).

During a ransomware attack, malware is injected into a network to infect and encrypt sensitive data until a ransom amount is paid.

Ransomware attacks are a growing threat amongst healthcare providers according to an analysis last year. More than 1 in 3 healthcare organizations globally fell victim to a ransomware attack in 2020.

The reason for its prevalence is that hackers understand how critical it is for the healthcare sector to minimize operation disturbances. During a ransomware attack, healthcare victims panic, fearing the regulatory consequences that follow the theft of patient data. Data Breach Investigations Report (DBIR).

Phishing: Like all industries, healthcare is at risk from phishing. According to Data Breach Investigations report (Verizon, 2023)[xviii] around 66% of malware was initiated as an email attachment. Although the WannaCry ransomware was unlikely to have begun its life in an email, much malware continues to be executed via phishing. However, phishing emails and texts are also a threat to personal data, including login credentials.

The National Health Information Sharing and Analysis Center have recently reported that the healthcare industry is at the most risk of fraudulent emails. However, little is being done to combat this, with 98% of healthcare organizations not taking the first steps in helping to prevent phishing by setting in place Domain-based Message Authentication, Reporting & Conformance (DMARC).

Insider threats: Insider threats to hospital resources are a concern across the board and can be carried out by patients as well as staff and can be both malicious and accidental. The HIMSS Cybersecurity Survey (2017), found that Insider threats were deemed to be worrying enough to set up specific programs of protection by 75% of respondents.
Spoofing: Spoofing is when someone hides their identity to evade detection for their wrong acts and pretends to be someone else in an attempt to gain trust and get sensitive system information. The common spoofing done by changing the hardware or MAC address is called MAC cloning, changing the IP address or the unique identity on the network is called IP spoofing, and impersonating as someone else in their digital communication is called email spoofing.

Information-gathering attacks: Information gathering is the practice of attacker gaining priceless details about probable targets. This is not an attack but only a pre-phase of an attack and is totally passive as there is no explicit attack. Systems including computers, servers, and net-work infrastructure, including communication links and inter networking devices, are sniffed, scanned, and probed for information like whether the target system is up and running, what all ports are open, details regarding the operating system and its version, etc. Some of the information-gathering attacks are sniffing, mapping, vulnerability scanning, phishing, etc.

Password attacks: The simplest way to achieve control of a system, or any user account, is through a password attack. If the personal and behavioral details of the victim are known, the attacker starts with guessing password. Frequently, the attacker uses some form of social engineering to trace and find the password. Dictionary attack is the next step in password attacks and is automated.

Virus: Computer viruses are the most communal threat to the computer users. Computer viruses are malicious software designed to blow out from one computer to another through file transfer, piggybacks on genuine programs and OS, or e-mails. The email attachments or downloads from particular websites contaminate the computer and also other computers on its list of contacts by using the communication network. Viruses influence the system security by changing the settings, accessing confidential data, displaying unwanted advertisements, sending spam to contacts, and taking control of the web browser According to Thomas C. (2009), the viruses are identified as executable viruses, boot sector viruses, or e-mail viruses.

Worms: Computer worms are fragments of malicious software that reproduce swiftly and blow out from one computer to another through its contacts, again spreading to the contacts of these other computers and so on and reaching out to a large number of systems in no time. Captivatingly, worms are prepared for spreading by exploiting software vulnerabilities. Worms display unwanted advertisements. It uses up tremendous CPU time and network bandwidth in this process thereby denying access to the systems or network of the victim, creating chaos and trust issues on a communication network.

Trojans: Trojans are programs that appear as perfectly genuine but, in reality, have a malicious part embedded in it. Trojans are spread usually through email attachment from the trustworthy contacts and also on clicking on fake advertisements. The payload of Trojans is an executable file that will

install a server program on the victim's system by opening a port and always listening to that port whereas the server is run on the attacker's system. Hence, whenever the attacker wants to login to the victim machine, they can do so by means of the backdoor entry making it hidden from the user.

Spyware and adware: Spyware and adware are software with a common property of collecting personal information of users without their knowledge. Adware is intended to track data of the user's surfing behaviors, and, based on that, pop-ups and advertisements are displayed. Spyware on the other hand gets installed on a computer and gathers information about the user's online activities without their knowledge. Spyware contains key loggers that record every-thing typed on the keyboard, making it unsafe due to the high threat of identity mugging.

Botnets: A collection of compromised systems or bots acts as a team of infected computers under the control of a bot master to remotely control and send synchronized attacks on a victim host. This army of bots, agents, and bot master constitute a botnet. Botnets are used for sending spams and also for distributed denial of service attacks.

Denial-of-service attacks: Denial-of-service (DoS) attacks as the name suggests denying users from accessing or using the service or system. This is mainly done by overwhelming the bandwidth, CPU, or memory wherein the access to the network of the victim machine or server offering the service gets denied. DoS attacks thus interrupt the service of a computer or network systems, making it inaccessible or too inferior in performance.4.16 Distributed DoS In distributed DoS (DDoS) attacks, the victim is targeted from a large number of individual compromised systems simultaneously. The DDoS attacks are normally done with the help of botnets. The botmaster is the attacker who indirectly attacks the victim machine using the army of bots or zombies. DDoS attacks occur when a large number of compromised systems act synchronously and are being coordinated under the control of an attacker in order to totally exhaust its resources and force it to deny service to its genuine users. It is the upsurge in the traffic volume that loads the website or server causing it to appear sluggish (Thomas C. 2009)

3. FACTORS INFLUENCING SYSTEM SURVIVABILITY ATTACKS IN HEALTHCARE.

Top Management should be responsible for informing their employees of the importance of systems survivability, make it efficient for people to participate, take ownership and manage their responsibilities (Abbas *et al*., 2015)[xix]. They also ought to invest in a solution that benefits everyone and finally monitor performance. Further, organizational resources come in whereby organizations lack industry expertise on survivability attacks resulting from a general lack of technology and the prohibitive expense of security personnel.

Game theory models the attacker and system administrator*'*s fundamentally selfish and aggressive actions and analyzes the potential strategies bringing in the human aspect of cyber security (Shiva & Sankardas, 2010). Securitization theory suggests there is currently a general perception that there is a lack of awareness and information in Kenya on systems security matters, leading to IT literacy as an individual factor. For systems survivability, intersectionality can help us better understand how system attacks issues are not just technical but are both legal and governmental, and cultural and economic, and so on which leads to policy formulation of IT policies for cyber security.

Based on the above from the literature review, the researcher aimed at reviewing organizational and individual factors, coupled up with mediating factors to come up with a framework for system survivability. From this, the researcher aimed to develop and validate a framework that addresses the human factors, organizational culture, and IT policies side of system survivability in the health sector.

Increased use of Cloud computing and online security

Cloud computing is being taken up by healthcare as it offers benefits such as improved access to data and cost efficiency. The use of Cloud computing within healthcare is set to soar, however, cloud computing brings its own risks (I Kravchenko, 2021). Data within cloud repositories need to be

correctly protected, according to Open Web Application Security Project (OWASP) guidelines. Protecting data at rest and during transit across web services requires not only robust encryption measures but also appropriate and effective authentication, such as second factor and risk based.

Internet-enabled healthcare attacks (Internet of Things - IoT devices)

Healthcare has embraced Internet-connected devices in a bid to use health data to improve patient outcomes. Apps like OpenAPS which are an optimized data-driven insulin delivery system and internet enabled activity trackers which help in cancer treatment are paving the way for the IoT to improve healthcare. However, the IoT has known security and privacy issues. Many healthcare based IoT devices aggregate personal data which is then stored in a cloud repository and used to analyze conditions, treatments, among others. Security issues such as DDoS attacks like the massive Mirai Bot (NJCCIC, 2016), which are based on IoT devices, are a potential threat that could disrupt treatment. The protection of personal data to prevent exposure is another. Redundancy issues are also another area of concern, as more hospitals become dependent on Internet-enablement of systems.

Lack of Data Encryption

Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and understands the gravity of losing it which is why HIPAA compliance requires every computer to be encrypted (Thakur, K., Hayajneh, T., & Tseng, J. 2019)[xx]

4. CONCLUSION

Some of the survivability crimes and threats are wrongdoing that are executed utilizing PCs or are in any case identified with them. Access to boundless information over the world is great yet it accompanies its reasonable portion of issues. In this paper, we have explored the principal vulnerabilities and risks that target health systems survivability and proposed a comprehensive system survivability model to address these challenges. Through the analysis of a case study and a review of relevant literature, we have developed a model that can be adopted for use as a strategy to overcome. By adopting this model, organizations can enhance their ability to identify and mitigate vulnerabilities in their environment, thereby improving their overall security posture.

5. REFERENCES

1. [i]. Farrukh Khan, Raymond A. Paul, 2012. In Advances in Computers, M
2. [ii] Shenoy, A., & Appel, J. M. (2017). Safeguarding Confidentiality in Electronic Health Records. *Cambridge quarterly of healthcare ethics : CQ : the international journal of healthcare ethics committees*, *26*(2), 337–341. https://doi.org/10.1017/S0963180116000931
3. [iii] Experts, A. U. (2018). *Call for Experts.*
4. [iv] Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66–72.
5. [v] Index, M. M. (2016).
6. [vi] Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and Security in Mobile Health: A Research Agenda. *Computer*, *49*(6), 22–30. https://doi.org/10.1109/MC.2016.185
7. [vii] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.
8. [viii] Whitler, Kimberly & Farris, Paul. (2017). The Impact of Cyber Attacks on Brand Image: Why Proactive Marketing Expertise Is Needed for Managing Data Breaches. Journal of Advertising Research. 57. 3-9. 10.2501/JAR-2017-005.
9. [ix] Scott, M., & Wingfield, N. (2017). *Hacking attack has security experts scrambling to contain fallout*. New York, USA: New York Times.
10. [x] Coventry, Lynne & Branley-Bell, Dawn. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 113. 10.1016/j.maturitas.2018.04.008.

11. [xi] Storm, D. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks*. London, UK: Computerworld.
12. [xii] Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurgery*, *92*(1), 454–462.
13. [xiii] Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143–1147.
14. [xiv] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.
15. [xv] Krisby, R. M. (2018). Health care held ransom: modifications to data breach security & the future of health care privacy protection. *Health Matrix*, *28*(1), 365.
16. [xvi] Pope, J. (2016). Ransomware: minimizing the risks. *Innovations in Clinical Neuroscience*, *13*(11–12), 37-41.
17. [xvii] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-12.
18. [xviii] Data Breach Investigations report (Verizon, 2023
19. [xix] Abbas, A., Bilal, K., Zhang, L., & Khan, S. U. (2015). A cloud-based health insurance plan recommendation system: A user centered approach. *Future Generation Computer Systems*, *43*(1), 99–109.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 8 – 20 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

A PROCESS FLOW MODEL FOR DYNAMIC ENTERPRISE NETWORK CYBER SECURITY ANALYSIS IN EASTERN AND CENTRAL UGANDA

Shariff MUGOYA[1], Twaibu SSEMWOGERERE[1], Godfrey ODONGTOO[1], Mwase ALI[2], and Gilbert Gilibrays OCEN[1]

[1]Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University, P.O. Box 236, Tororo, Uganda

[2]Department of Marketing and Management, Makerere University Business School, P.O. Box 1337, Kampala, Uganda

ABSTRACT: Several Enterprises are adopting Enterprise Networks due to their benefits like remote file storage, resource sharing, and improved communication. Due to a large number of target groups, cyber-attackers have exploited vulnerabilities in the Enterprise Networks to launch cyber-attacks on these networks thus resulting into data theft and financial losses to the enterprises. In this study a Dynamic Enterprise Network Cyber Security Analysis Model that considers the ever changing components of enterprise networks was developed and implemented on windows operating system. Purposive sampling was used to select key informants with technical knowledge about cyber security. Primary data was collected using closed-ended questionnaires and secondary data was collected from analysis of scholarly articles, books, conference papers, and journals. Expert opinion guided the testing and implementation of the developed model.

KEYWORDS: Enterprise networks, Cyber Security, Analysis Model, Dynamic

1. INTRODUCTION

Of recent the use of smart phones, internet and computers is so popular in our lives. This is both for individuals and organizations. As of 2024 there were 5.35 billion internet users worldwide which is 66.2% [1] and according to [2] there are 6.93 billion smartphone users worldwide.

Organizations and enterprises have embraced networking of Computers thus coming up with Enterprise networks. This is attributed to the benefits like resource sharing, remote file storage, and improved communication that come with the networking of computers. However, since access to the server computer affects activities of all computers on the network, cyber-attackers have highly targeted networked computers by exploiting network vulnerabilities thus plunging enterprises into huge financial losses and data losses. Most of the attacks have been as result of errors on the enterprise employees' part.

Cyber-attacks can lead to significant financial losses for large enterprises. The exact amount of losses varies depending on various factors such as the nature of the attack, the size of the organization, the industry sector, and the effectiveness of the organization's security measures. Some notable examples of large enterprises and the losses they have experienced due to cyber-attacks include;

In 2013, Target, a major U.S. retailer, suffered a cyber-attack that compromised payment card information of approximately 40 million customers. The attack also exposed personal information of around 70 million customers. The breach cost Target an estimated $162 million, including expenses related to investigation, remediation, legal fees, and settlements [3].

In 2014, Sony Pictures Entertainment experienced a highly publicized cyber-attack attributed to North Korea. The attack resulted in the theft and release of sensitive company data, including employee information and unreleased films. Sony Pictures estimated the total cost of the attack to be approximately $15 million, including remediation efforts, investigation, and legal fees [4].

In 2017, Equifax, one of the largest credit reporting agencies, experienced a massive data breach that exposed personal information of approximately 147 million people. The breach resulted in significant

financial losses for Equifax, including legal settlements, remediation costs, and damage to its reputation. The estimated total cost of the breach exceeded $1.4 billion [5].

In 2017, Maersk, a global shipping company fell victim to the NotPetya ransomware attack, which affected its IT infrastructure worldwide. The attack resulted in significant disruptions to Maersk's operations, including the shutdown of critical systems and the loss of data. The company reported losses of around $300 million due to the incident [6].

According to the Police Crime report for 2020, Shs. 15 billion was lost through cyber fraud. According to NITA-U, the fraud mostly targeted mobile money and bank operated internet services [7].

It's important to note that these are just a few examples, and the financial impact of cyber-attacks on large enterprises can vary widely. Additionally, the true cost of a cyber-attack may extend beyond immediate financial losses, including reputational damage, customer loss, and regulatory fines.

In a bid to mitigate such attacks enterprises have employed solutions like basic cyber security trainings for all employees, password rotations, 2 factor authentication, and password security policies but in vain.

Due to an increase in situations like cyber-attacks, civil and criminal proceedings, and other industry events, process models were presented and created [8] to address the challenge of Enterprise Network Cyber Security vulnerabilities for example Attack Tree model [9], Attack Graph model [10], STRIDE model and many others. However, the limitation to these models and the aforementioned enterprise solutions is that they work for static networks yet most of the enterprise networks currently are dynamic i.e. the load on the network changes over time, packets to be route come and go, objects in an application are added and deleted constantly, more workstations are constantly added to the network with the increase in the number of employees.

According to [11], the graphical security model-based analysis which would offer a fair solution has several problems that need to be addressed and future research in the areas of adaptability, scalability, and lack of empirical data is suggested. This renders the existing enterprise network security models ineffective.

With such prolific increase in malware attacks targeting Enterprise Networks due to presence of many network vulnerabilities in them which are exploited by cyber-attackers, there is a need to have an Enterprise Network with up-to-date cyber security risk countermeasures. Therefore the major contribution of this study is to develop a Cyber Security Analysis Model that caters for dynamic networks.

2. METHODOLOGY

The methodology that was applied in this research is Design Science Research (DSR). This is due to the fact that DSR is a commonly used and recognized method of producing artifacts in the field of information systems research. It provides a methodical framework for creating objects like constructs, models, procedures, or instances. As a result, it is suitable for designing a DENCAM. DSR is also useful for identifying and implementing feasible solutions within a challenging context [12].

In designing a DENCAM, the following six (6) steps of DSR were followed:

Step 1: Identify the problem and Motivate.

There is an increase in Enterprise networks as a result of several attacks targeting Enterprise Network Systems. Therefore there is need to increase security of the Enterprise Networks such that they are more resistant to such attacks.

Step 2: Define the Objectives

To analyze the security of Enterprise Networks.

To enhance the security of Enterprise Networks.

To simulate several attacks on enterprise networks and observe how the networks counteract them.

Step 3: Design and Development

SolarWinds ipMonitor network monitoring tool was used to monitor the changes in the network components. The new changes in the network components were noted.

MITRE ATT & CK matrix was used as a knowledge base to identify cyber threats to the network and mitigate them. More emphasis was put on the new changes on the network.

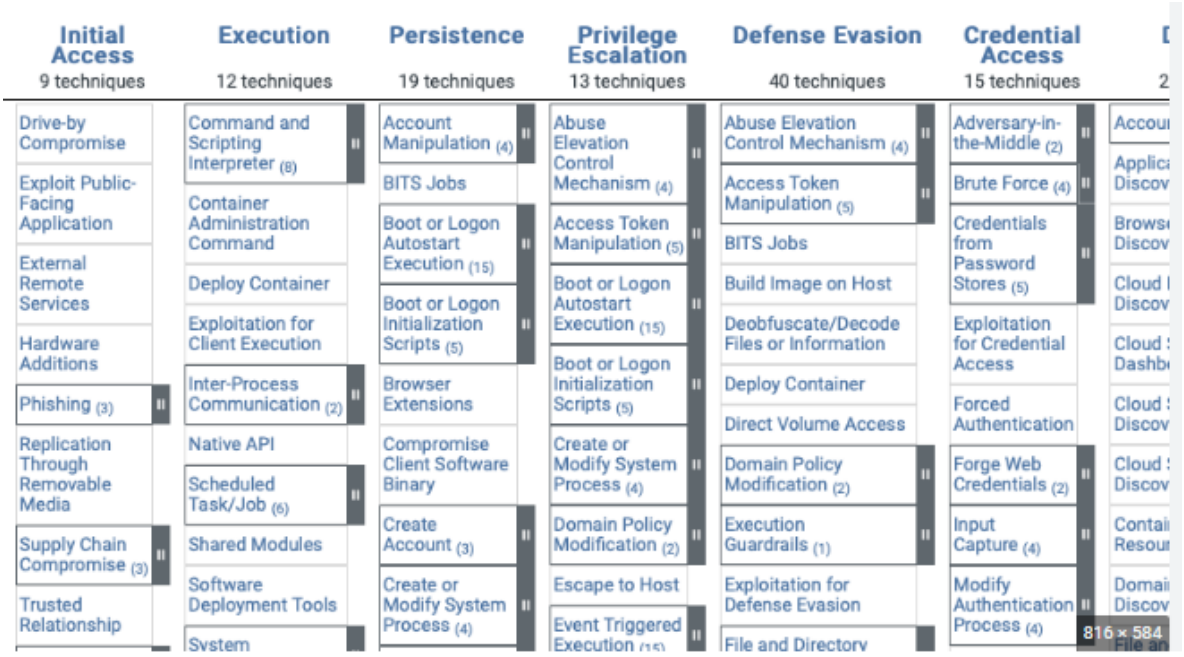


Fig.1. *MITRE ATT & CK matrix*

Step 4: Demonstration
Simulation attacks were launched on the enterprise network using Cymulate threat emulator.
Step 5: Evaluation
The response to the attacks by the Enterprise Network was noted and the Enterprise Network observed to see whether it has behaved as expected.
Mitigations to the Enterprise Network security were put in place for instance security settings of the system will be enhanced to combat such threats in the future.
Step 6: Communication
The research findings were communicated through publishing them.
2.1. Study Area and Period. The study was carried out in Eastern and Central Uganda in the districts of Wakiso, Jinja, Mukono, Buikwe, Iganga, Luuka, and Busia. The study was carried out for a period of 16 months from September 2022 to December 2023.
2.2. Sampling Strategy and Sample. Purposive sampling strategy was used on 56 respondents from 10 enterprises with Enterprise Networks. This is because the required data had to be got from specific Enterprise Network stake holders. In the sample enterprises, Enterprise Managers, Enterprise Network administrators, Enterprise Network users, and Enterprise technicians were targeted.
2.3. *Data Collection Methods*. Survey using semi-structured questionnaires were used to gather data about Enterprise Network stakeholders, and the Enterprise Networks themselves. This is because such questionnaires allow respondents to give detailed responses and also cater for the varying levels of expertise of the respondents. Experimentation data collection method was used to demonstrate the readiness of the Enterprise Networks to combat cyber threats.
2.4. *Data Analysis and Presentations*. Qualitative data was analyzed using Qualitative Content Analysis method because it evaluates patterns within a certain piece of data; and also can be used to identify the frequency with which an idea is shared by the respondents. Quantitative data was analyzed using SPSS tool because it can be used to identify trends, develop predictive models, and also to draw informed conclusions.

2.5. Ethical Consideration. Informed consent; the selected respondents and study population were informed of the study and gave their consent before the study commenced. Voluntary participation; participants in the study voluntarily accepted to participate in the study without coercion or duress. Do not harm; the study and the outcomes of the study were designed in a way that they do not harm the study population. Confidentiality; sensitive information about the sample population was and will never be revealed. Anonymity; the identities of the respondents and sample enterprises were concealed.

2.6. Environmental and Gender implications. This study had minimal negative impact on the environment since the survey questionnaires used were collected after the study for recycling. Also at the end of the study a tree was planted at each of the sample enterprises to help reduce on the carbon dioxide content in the atmosphere. Gender equality and equity was a major determinant in selecting respondents in this study.

2.7. Model Development

2.7.1. Steps in the model. The process of developing the model starts by checking whether the device being analyzed is powered on. If the device is not powered on, then it should be powered on. Once it is confirmed that the device is powered on, it is then checked for network connectivity. The device should be networked if not, then it should be connected to a network. Not just any network but the network of the enterprise in which the device belongs. SolarWinds ipMonitor (Network monitoring tool) is then run to start monitoring the Enterprise Network for changes in its components. Once there are changes, the anomalies and threats are detected MITRE ATT & CK provides the required up-to-date threat knowledge. Lastly, incident Response is immediately implemented as shown in figure 2 below.

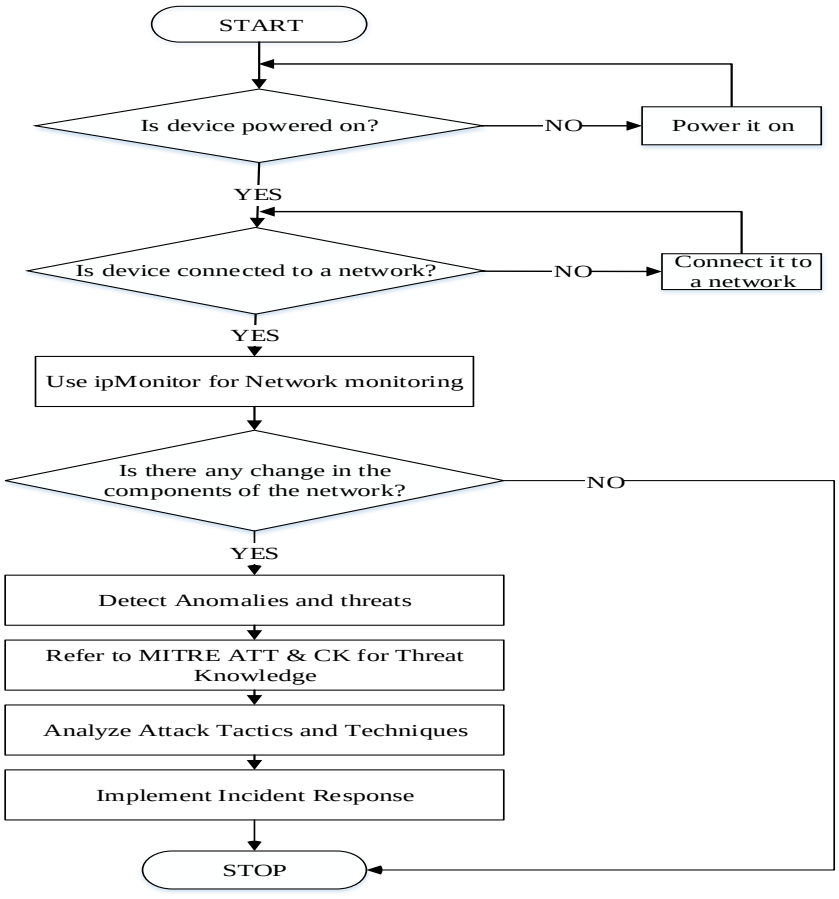


Fig.2. *Dynamic Enterprise Network Cyber Security Analysis Model*

2.8.2. Experimentation. The device being analyzed for Cyber Security threats was powered on and it was ascertained that it was connected to its Enterprise Network. SolarWinds ipMonitor network monitoring tool was used to determine the changes in the components of the network. The interface Solarwinds ipMonitor was as shown in figure 4 below.

3. RESULTS AND DISCUSSION

3.1. Demographic Characteristics. 67 questionnaires were sent to the field of study, however, only 56 were returned fully answered representing a response rate of 83.58%. 58.9% males and 41.1% females responded to the survey; 39.3% of the respondents are in the age bracket of 20 – 39 years while 1.8% in the age bracket of 50 – 59 years. Most of the respondents were from government enterprises representing 62.5% and the remaining 37.5% from private enterprises. 67.9% of the respondents have university degrees while 1.8% have certificates.

3.2. Validity Test. Content Validity Test was used to determine the validity of the questionnaire. Experts were consulted and on examining the tools agreed that 80% of the questions raised can help achieve the objectives of the study. In order to examine the validity on each of the constructs rated against Enterprise Network Cyber Security factor analysis, Principal Component Analysis with varimax rotations was used and the results for each construct were desired and satisfied the analysis as shown in tables 2, 2, and 3 below. KMO was used to determine whether the responses given by the sample are adequate or not. 0.5 is the recommended minimum (barely accepted) KMO value [13]. All responses satisfied this condition as shown in tables 4, 5, and 6.

Tab.1. *Component Factor Loading on the construct of Vulnerabilities*

Component Matrix[a]

	Component 1
Availability of a formal incident response plan	.747
Biggest Cyber Security challenges for the organization	.747

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.2. *Component Factor Loading on the construct of Threat* Intelligence and Detection

Component Matrix[a]

	Component 1
Ways of Handling Security incidents/breaches	.902

Frequency of vulnerability assessment testing	.902

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.3. *Component Factor Loading on the construct of Security Controls*

Component Matrix[a]

	Component 1
Rating of organization's network security measures	.831
Number of times security awareness training is conducted	.724
Source of latest Cyber Security threats and trends	.634
Security measures in place	.385

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.4. *KMO value for Vulnerabilities*

KMO and Bartlett's Test for Vulnerabilities

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	.715
	df	1
	Sig.	.398

Tab.5. *KMO value for Threat Intelligence and Detection*

KMO and Bartlett's Test for Threat Intelligence and Detection

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	26.935
	df	1

	Sig.	.000

Tab.6. *KMO value for Security Controls*

KMO and Bartlett's Test for Security Controls

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.582
Bartlett's Test of Sphericity	Approx. Chi-Square	23.334
	df	6
	Sig.	.001

3.3. Reliability Testing. According to [14], reliability is the extent to which a questionnaire provides consistent results. That is to say the ability of a questionnaire to obtain true information. The questionnaires were pre-tested using a small sample population which was not included in the study. Test-retest reliability test was used to determine the consistence of the questionnaire. Cronbach's Alpha test for internal consistence was used on each item of the instrument. Cronbach's Alpha value of 0.653 was obtained which according to [15] is moderate reliability thus making the items of the instrument consistent.

Tab.7. *Reliability statistics*

Reliability Statistics

Cronbach's Alpha	N of Items
.653	16

3.4. SWOT Analysis. The SWOT analysis was done by analyzing related literature about Enterprise Network Cyber threat models and comparing the developed model with the existing models. Table 8 below shows the results from the comparisons.

Tab.8. *Comparison of the developed (DENCAM) with the existing models*

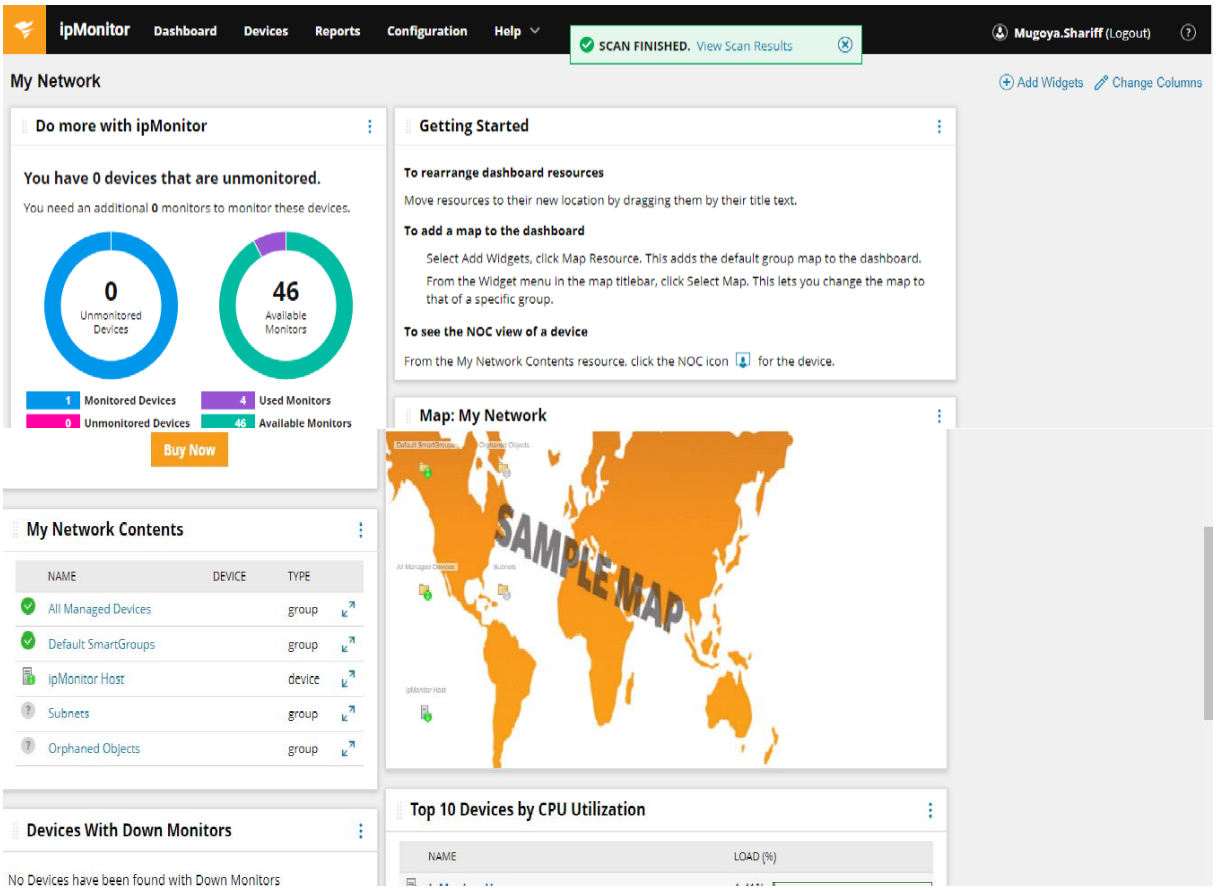
Model	Ability to detect new threats	No false positives	Caters for scalable networks	Caters for Dynamic networks
Signature-based detection	X	X	X	X
Anomaly-based detection	✓	X	X	X
Behavior-based detection	✓	X	✓	X
Machine learning-based detection	✓	X	X	X
Intrusion Detection Systems (IDS)	X	X	X	X
Intrusion Prevention	✓	X	X	X

Systems (IPS)				
Network Traffic Analysis (NTA)	✓	X	X	X
Security Information and Event Management (SIEM)	X	X	✓	X
Threat Intelligence Platforms	✓	X	✓	X
User and Entity Behavior Analytics (UEBA)	✓	X	✓	X

3.5. Experimentation

The device being analyzed for Cyber Security threats was powered on and it was ascertained that it was connected to its Enterprise Network.

SolarWinds ipMonitor network monitoring tool was used to determine the changes in the components of the network. The interface Solarwinds ipMonitor was as shown in figure 3 below.



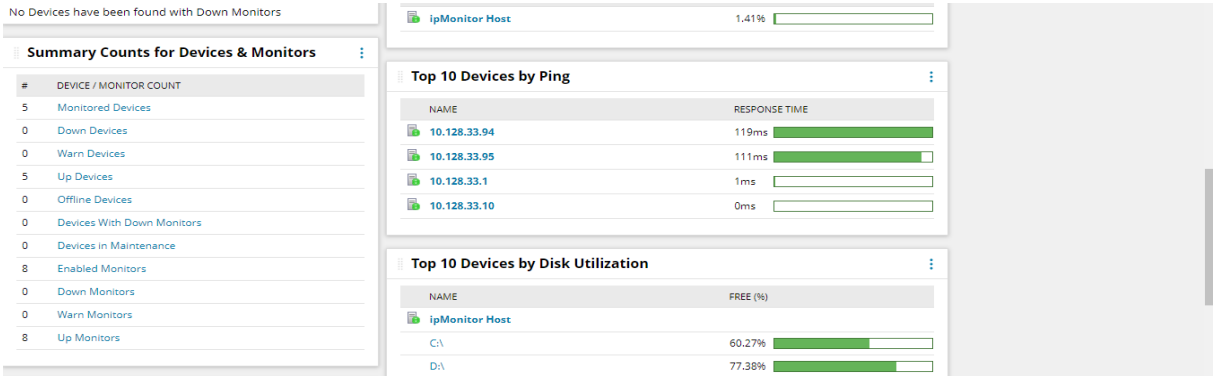


Fig. 3: *Beginning interface of SolarWinds ipMonitor*

Cymulate threat operator was used for simulation attacks. The SolarWinds ipMonitor scanned all the devices in the Enterprise Network and the results were as shown in figure 4 below.

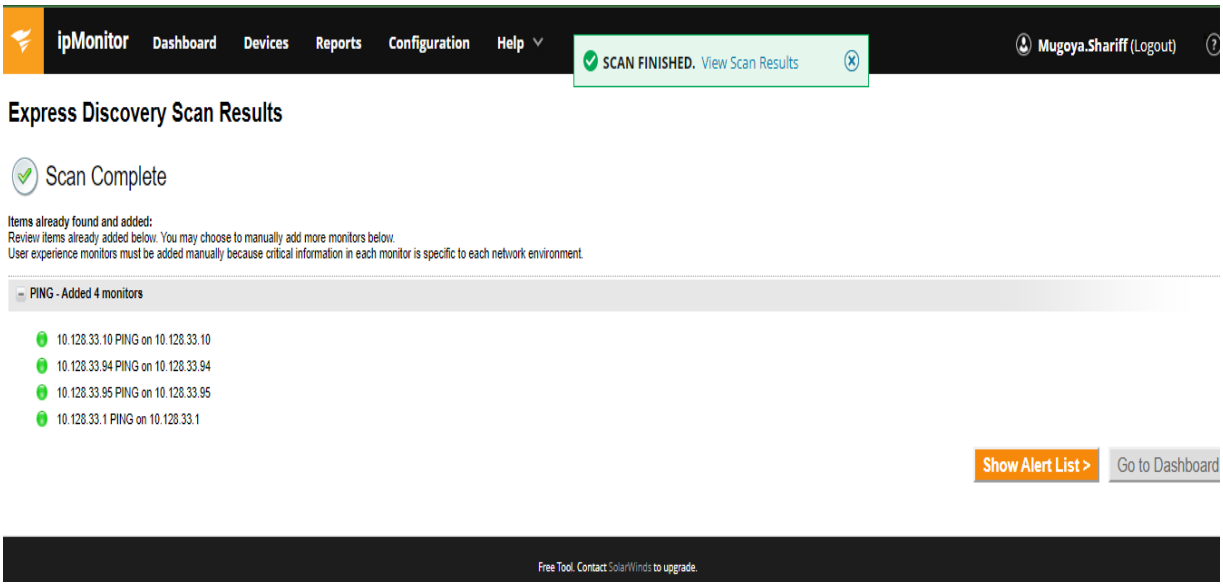


Fig. 0: *Results of Scan*

4 monitors were added to the network making it a total of 46 monitors in the Enterprise Network as shown in figure 4 above.

Scan results for each of the devices in the enterprise Network were as shown in figure 5 below.

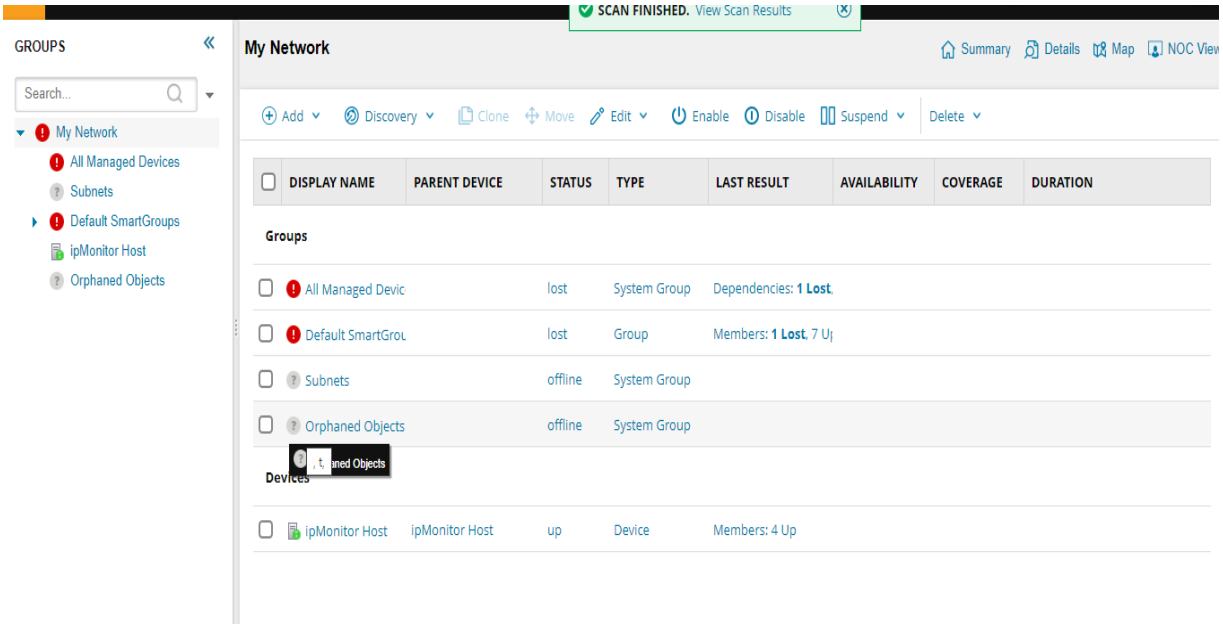


Fig. 5: *Scan Results for the whole network*

The scan results for the Host device was as shown in figure 6 below.

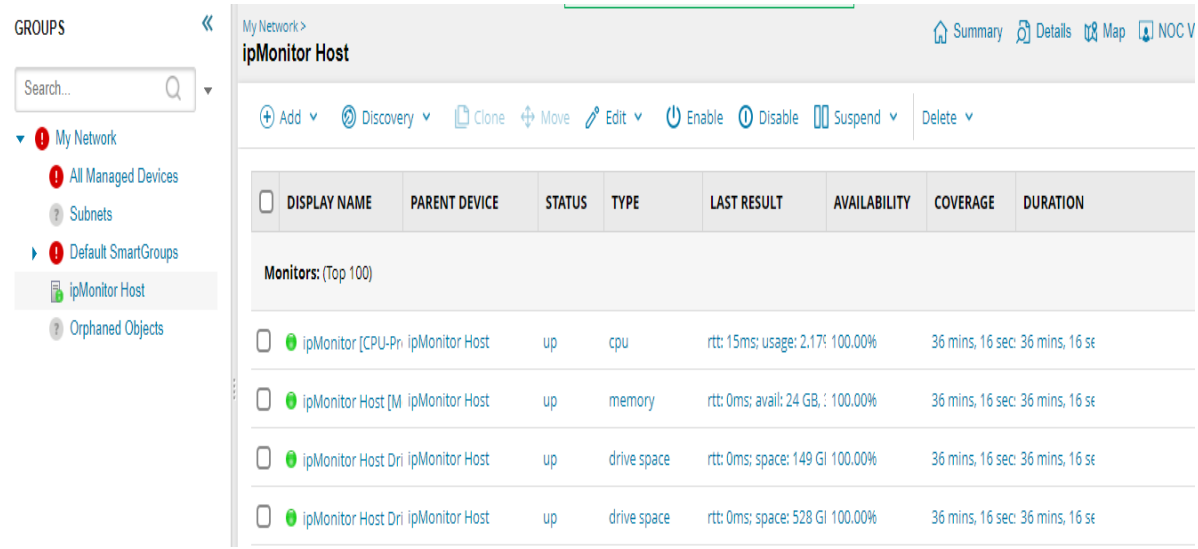


Fig. 6: *Scan Results for Host device*

Report from the scan of the whole network for changes in its components were given as shown in figure 7 below.

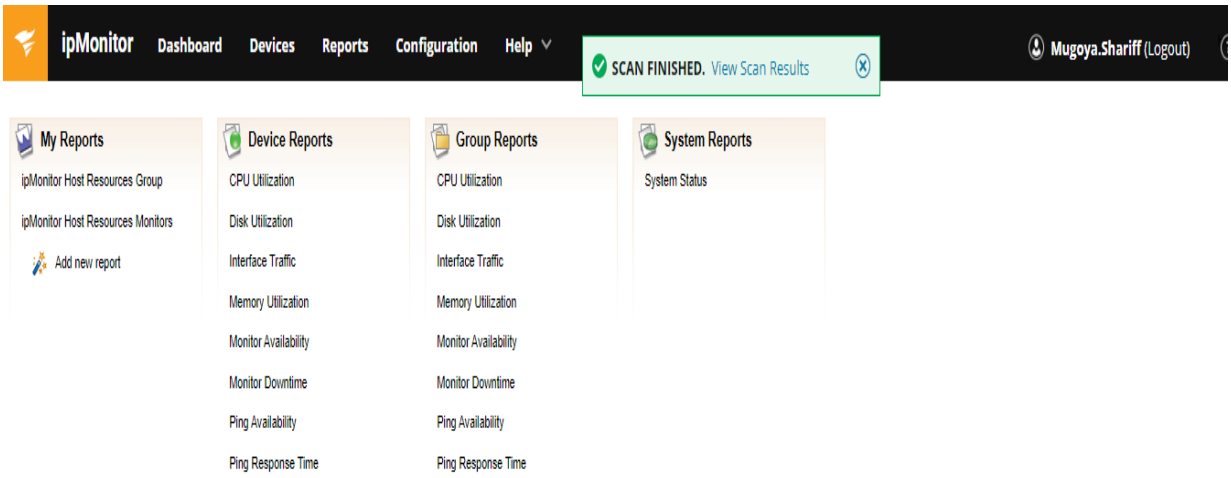


Fig. 7: *Scan Report for the Enterprise Network*

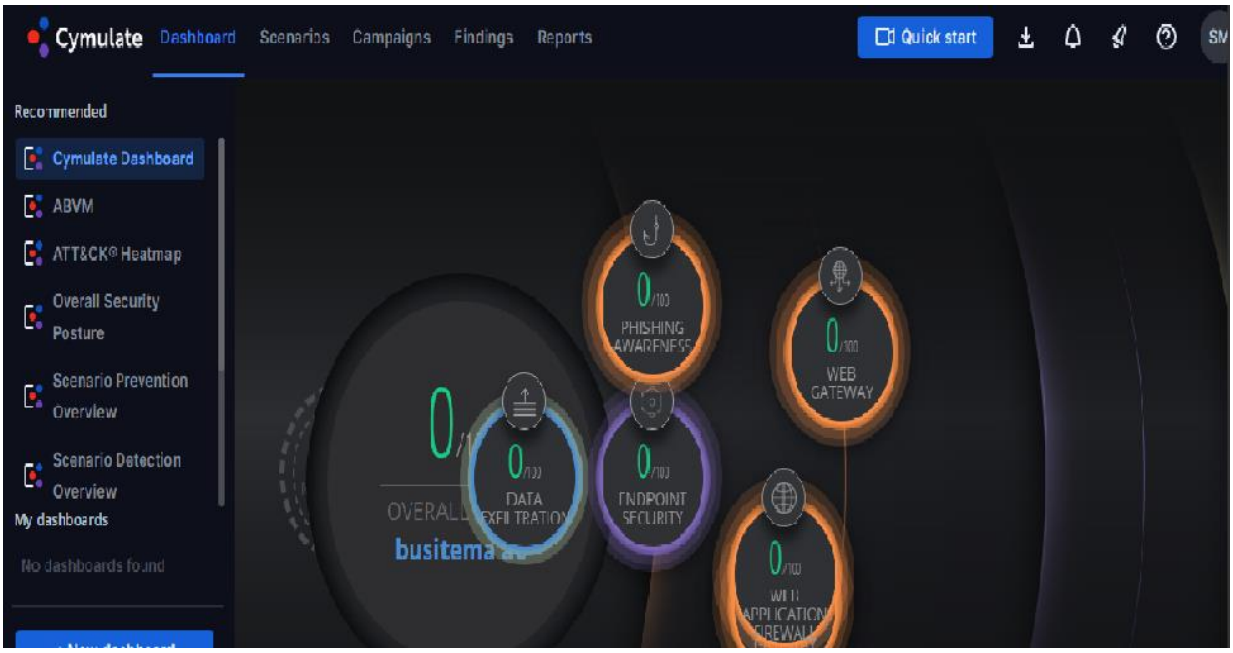


Fig. 8: *Cymulate dashboard*

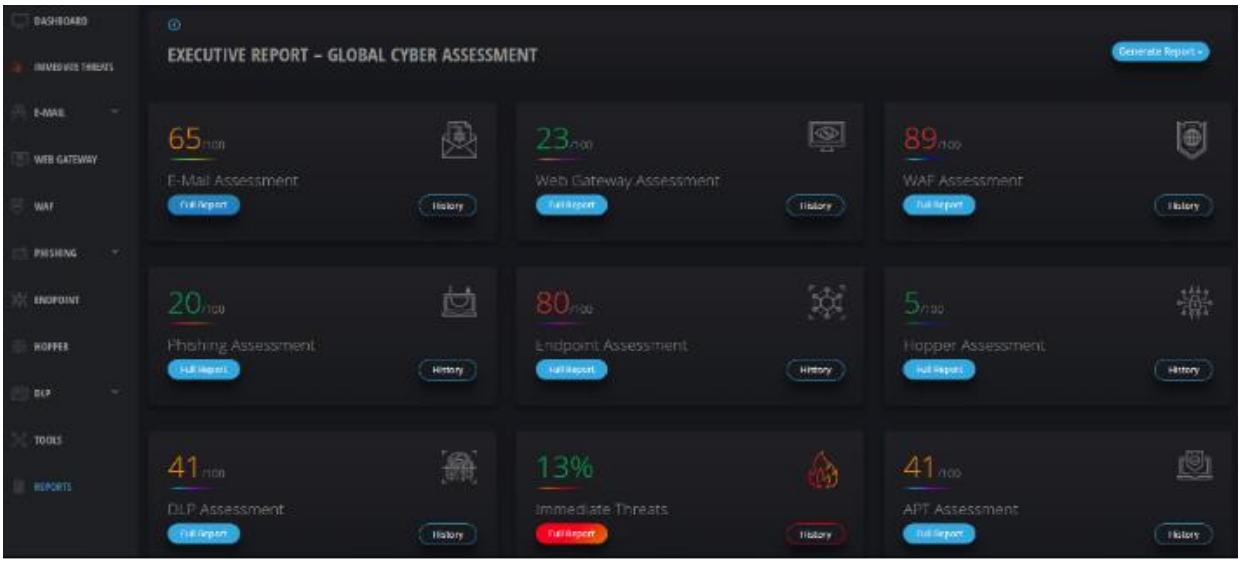


Fig. 9: *Cymulate Simulation report*

4. CONCLUSION AND RECOMMENDATIONS

In this study, an Enterprise Network Cyber Security Analysis Model that considers the constant changes that occur in the components of the network (DENCAM) has been developed. It uses network monitoring tools (e.g. SolarWinds ipMonitor) to monitor the changes in the components of the network, then uses MITRE ATT & CK as a knowledge base for the latest cyber threats and how to combat them. The Incident Response recommended by MITRE ATT & CK is then implemented. The model was tested and validated through experimentation.

Future research should focus on developing a model that can be applied on all operating systems besides Windows operating system.

REFERENCES

1. Statista. (2024). Internet user population. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/ Accessed on January 16th, 2024, at 4:30 P.M.
2. HOW MANY SMARTPHONES ARE IN THE WORLD? (2024). Retrieved from https://www.bankmycell.com/blog/how-many-phones-are-in-the-world. Accessed on January 17th, 2024, at 8: 16 A.M.
3. M. McGrath (2014). Target Data Breach Spilled Info On As Many As 70 Million Customers. Retrieved from https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=df3f7cce7954. Accessed on January 17th, 2024, at 8:29 A.M.
4. A. DeSimone, and N. Horton. (2015). Sony's Nightmare Before Christmas.
5. M. Hill (2023). The biggest data breach fines, penalties, and settlements so far. Retrieved from https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html. Accessed on January 17th, 2024, at 8:46 A.M.

6. M. Mcquade. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ Accessed on January 17th, 2024, at 8:52 A.M.
7. Uganda Police Force. (2022). Annual Crime Report. Retrieved from https://www.upf.go.ug/
8. Ocen, G. G., et al. (2019). An Algorithm and Process Flow Model for Extracting Digital Forensic Evidence in Android Devices. International Scientific Journal Theoretical and Applied Science, 72(Issue 04).
9. Schrenier, B. (1999). "Attack trees." Dr. Dobb's Journal, 24(12), 21-29.
10. Phillips, C., & Swiler, L. P. (1998). A graph-based system for network vulnerability analysis (pp. 71-18).
11. S. Yusuf Enoch et al. (2021). Model-based Cyber Security Analysis: Past Work and Future Directions.
12. Bevan , J. L. , Tidgewell , K. D. , Bardull , K. C. , Cusanelli , L. , Hartsern , M. , et al. . (2007). Serial argumentation goals and their relationships with perceived resolvability and choice of conflict tactics.
13. H.F. Kaiser. (1974). An Index of Factorial Simplicity.
14. C.R. Kothari. (2004). Research Methodology: Methods and Techniques.
15. C. B. Perry R, Hinton, Isabella McMurray. (2014). SPSS Explained Second Edition.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 21 – 34 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MITIGATING THE IMPACT OF PHISHING ATTACKS ON THE E-LEARNING INFRASTRUCTURE

Mamman Ojima John[1], Onoja Emmanuel Oche[2], Enoch Blessing Toyin[3]

[1]Department of Mathematics, Federal University of Agriculture Makurdi

[2]Department of Cyber Security, Federal University of Technology Minna

[3]Department of Mathematics, Federal University of Lafia

ABSTRACT: An essential component of the educational system is e-learning. this study delves into the potential risks and threats that e-learning systems face from unauthorized access by third parties and ways to protect data from unauthorized use, alteration, and reuse in a variety of e-learning-related circumstances, this work presents a systematic literature review on phishing techniques. it also takes mitigation techniques for phishing into account. as a result, the component and the threat posed by the information security component are presented in this study. in addition, important information security techniques for safeguarding e-learning systems are suggested at the conclusion of this paper. today, cybercrime remains a continuous danger. this paper gives an overview of the different types of phishing attempts and how they work. we come across new forms of cybercrime every day, along with its dire repercussions. as a result, there are numerous ways for hackers to pilfer sensitive and important data in addition to money. we also provide ideas and tactics that should be taken into account while creating mitigation plans. mitigation strategies primarily rely on human-centric approaches, secure e-learning systems, machine learning and neural networks, deep learning, and cryptography. as new phishing attacks emerge, new strategies will continue to develop to counter them.

KEYWORDS. E-Learning; Phishing; cybercrime; threat; Security, Cryptography.

1.0 INTRODUCTION

There is seldom a week that goes by without news about hackers assaulting companies, governments, colleges, and people all across the world. If we were to learn about all these online crimes, we might decide to quit using the internet altogether, which would be extremely inconvenient for us. The current study's review is likewise predicated on (Das et al., n.d.) where the hazards are actual, albeit it can be challenging to gauge their scope. It's not always about stealing money; sometimes it's about stealing ideas. The scope of intellectual property (IP) theft on a global scale is unprecedented (Eze et al., 2018). E-learning platform have a particular issue with IP theft. Since educational systems frequently fall behind in terms of technology and qualified employees, they are soft targets for cybercriminals (Ennu et al., 2018). Security breaches of E-learning networks can have serious repercussions, costing colleges millions. This study's aim was to identify cyberthreats and the most likely places where online learning systems would be vulnerable to attack. Instead of fully avoiding the internet, it is crucial that we understand the many kinds of cybercrimes and how to prevent becoming a victim of them. According to (Drzani, 2014) a fundamental definition of cyber crime is any criminal activity involving the use of the internet or cyberspace as a means to carry out the intended dishonest conduct for financial gain or other forms of dishonesty. Cybercriminals target particular computers, the most prevalent cybercrimes today include pharming, phishing, skimming, eavesdropping, and DOS attacks. Phishing is a form of online fraud in which the attacker poses as a reliable source (Catal et al., 2022). The attacker uses temptations that the victim is likely to succumb to in an attempt to seduce them and sensitive information about the victims, including credit card numbers or login credentials is typically stolen by these attackers (Das et al., n.d.) and (Desolda et al., 2021). This occurs when the victim clicks on a link sent by an attacker posing as a legitimate entity or when they give information to the attacker over the phone. The intrusive party collects user information and utilizes it maliciously against the victim by seducing the victim and promising false rewards. Annually, there is a rise in security events and breaches that target the human aspect of cybersecurity. Phishing attacks are a popular type of cyberattack that prey on people's ignorance of

cybersecurity. Phishing occurs when a perpetrator deceives a target into doing an action that is detrimental to both the victim and the system. It also involves attempts made without authorization to pose as a reliable source in order to gain sensitive information. These definitions make it evident that phishing is a fraudulent endeavor, albeit the attackers' motivations differ. Typically, its goal is to obtain financial information, steal sensitive data, and get access to system credentials. Phishing is additionally utilized as a vector for other assaults, including ransomware attacks. Recently, phishing attacks have targeted businesses, with malware containment costs, lost productivity costs, credential containment costs, and ransomware costs looming in its path (Abdillah et al., 2022).

This paper is organized as follows. First, the introduction gives a brief summary of the significance of cybersecurity in today's digital world, with a focus on e-learning platforms. It increases public awareness of the frequency of cybercrimes and their possible impacts on people and businesses. To emphasize the importance of the issue, it also cites pertinent studies.

Materials and Methods contains a list of the selection criteria for research publications, databases consulted, search terms utilized, and platforms or frameworks for data extraction and analysis.

The meaning of our results and how they relate to earlier research are covered in the results and discussion section.

The conclusion highlights the importance of phishing attacks and summarizes the major findings of the research.

2.0 MATERIALS AND METHODS

This approach describes the systematic literature reviews (SLRs) of phishing techniques, Risks and threats associated with e-learning systems and mitigation strategies against phishing attacks. As phishing attacks become one of the top cyberattack trends, the research community has worked hard in order to lesson the difficulties caused by phishing assaults (Chen et al., 2022) and (Alaubaci et al., 2024). Consequently, numerous research publications have emerged, shedding light on various aspects of phishing phenomena, user responses, and potential remedies (Prosen et al., 2022) and (Nadeem et al., 2023). In recent years, a series of literature reviews (SLRs) have been conducted and published, serving as comprehensive summaries of existing knowledge and guiding future studies in this field (Dima et al., 2022) and (Altaher, 2021). Notably, the selection of research papers for this study employed the VOSviewer tool, which considers word clusters, frequency, and impact factors to facilitate data extraction. VOSviewer's user-friendly interface enables the identification of significant clusters of key terms, which in turn inform the grouping of research activities and subsequent publications exploring various data relationships. The sources utilized for bibliometric information include Web of Science, Pubmed, digital libraries, Scopus, and search engines like Google, all of which are highly reputable.

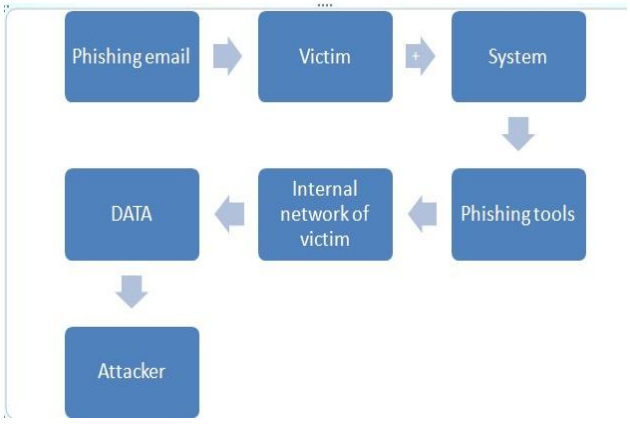


Fig. 1. *Process of phishing*

While numerous evaluations have recently been published, providing comprehensive descriptions of phishing attempts and encompassing both non-technical and technical protective measures, not all assessments have focused on the types and underlying reasons behind these attacks. The review

conducted by (Catal et al., 2022) highlights machine learning-based phishing detection techniques as its primary finding. This review thoroughly examines and evaluates strategies, information sources, records, feature selection methods, deep learning (DL) algorithms, assessment factors, verification methods, and the execution structures employed throughout the system's learning model life cycle. Additionally, the review identifies challenges associated with phishing detection and proposes potential solutions. The challenges and potential solutions are discussed in the review conducted by (Abdillah et al., 2022). The review focuses on the most common phishing assault vectors, sources of data, and detection methods employed to counteract phishing attempts. Additionally, the review examines the techniques utilized for rating performance in phishing attacks. The findings are presented in Table 1, which represents the Phishing Attack Incident from 2020 to 2022, as reported by Wise Online. The table provides information on the targeted industries and the percentage of phishing attacks in each industry for the years 2020, 2021, and 2022. Furthermore, Figure 2 illustrates the phishing attacks in the industry.

Tab.1. *Online report by Wise*

Targeted industry	2020	*2021*	*2022*
Webmail	29.80%	29%	29%
Financial	14.20%	15%	14.20%
Payment	33%	32.90%	33.90%
Logistics/Shipping	3%	3.20%	3.20%
Telecommunication	3.20%	3%	3%
Cloud Storage	4%	4.10%	4%
Others	12.80%	12.80%	12.70%

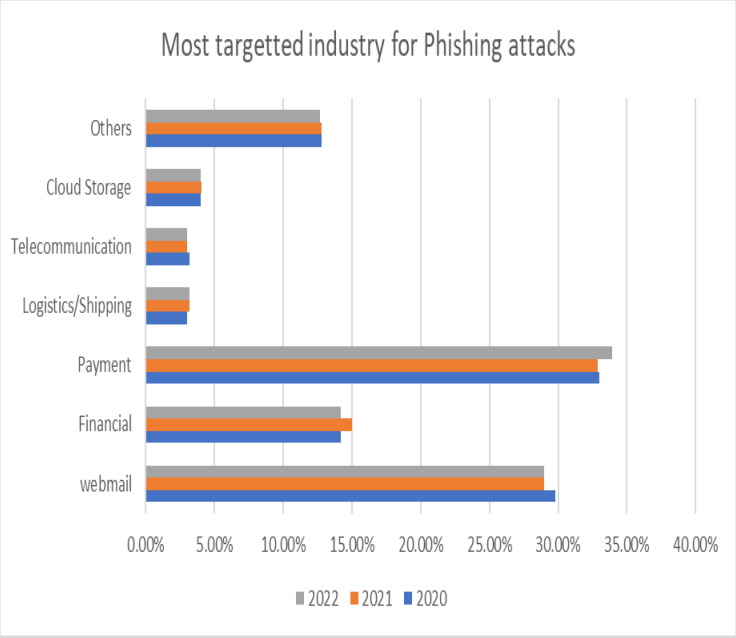


Fig. 2. *Wise online report of phishing attack incident from 2020 to 2022*

(Safi & Singh, 2013) conducted an examination of the literature on various methods for detecting phishing websites, information sets, and quantitative assessments of performance, including machine

learning-based methodologies. They also explored the use of natural language processing (NLP) to identify phishing emails and NLP-based methods for this purpose. (Desolda et al., 2021) and (Arshad et al., 2021) reviewed the literature on phishing and anti-phishing techniques, with a particular focus on the human element in phishing assaults. They discussed human-based ways to mitigate phishing attempts and user-based interventions.

Fig. 3*. Utilizing VOSviewer, a word cloud was created based on keywords from authors and index terms*

It is worth noting that the current classification schemes proposed by (Chanti & Chithralekha, 2019) and (Apandi et al., 2020) were not utilized in this literature review. These classification methods have limitations in classifying a wide range of data and are restricted to specific attack vectors. As a result, they are not applicable in the context of anti-phishing strategies. Furthermore, we examined the author keywords and index phrases for every publisher in order to find trends for categorizing anti-phishing tactics. To see the terms ranked by frequency, make a word cloud similar to the one shown in Figure 3. Figure 3 depicts the introduction of pertinent terminology for categorizing mitigation, including "algorithm," "system," "tool," and "learning." with regard to categorizing mitigation tactics. Still, they do not represent the entire taxonomy of mitigation techniques taken into account.

2.1 TECHNIQUES OF PHISHING

Middle-Man

This form of attack involves an unauthorized individual, known as the attacker, covertly intercepting the communication between the parties involved. The attacker gains illicit access to the transmitted information, manipulates it, and then forwards it to the intended recipient. As a result, the message is altered, and its original content is neither authentic nor genuine.

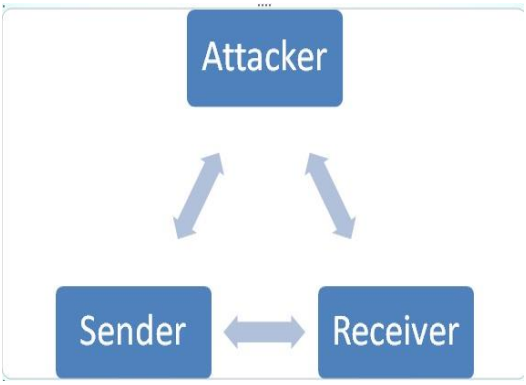


Fig. 4. *Middle-Man*

Email Phishing

Scams Attackers may go to great lengths to craft seemingly genuine emails to trick victims into providing the requested data (Sallaum et al., 2022). The attacker uses the original logo of the fake company and her signature to appear valid (Muutode & Parwe, 2019). Attackers also manipulate victims by mentioning urgency. For example, a phishing email could indicate that something is going on to pressure user to take necessary action as soon as possible. This leaves victims vulnerable and gradually becoming victims. Example as seen in fig. 5 below:

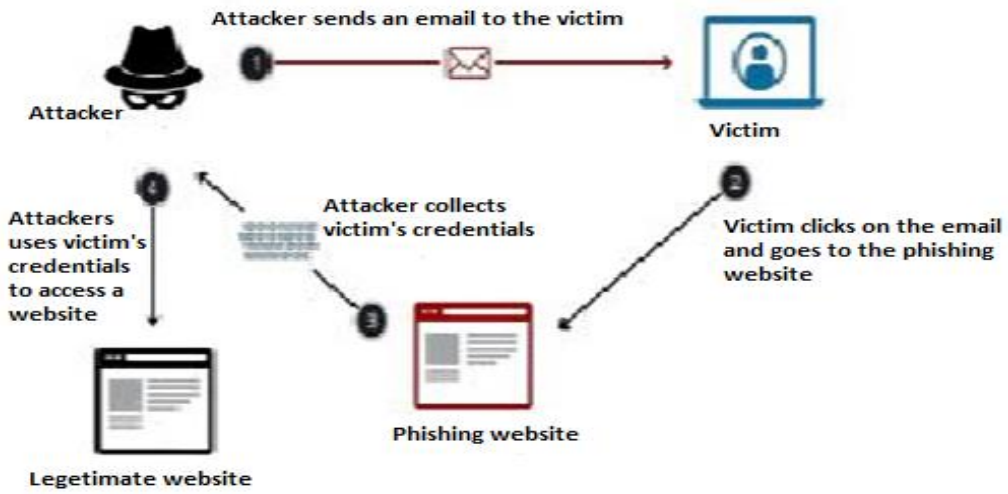


Fig. 5. *Example of e-mail Phishing*

Spear Phishing

Spear phishing involves targeted attacks directed at specific organizations or individuals for predetermined purposes (Ciangaxatapu et al., 2020). This technique requires in-depth knowledge of the target, including their operational structure. By tailoring the phishing attempt to the specific characteristics of the target.

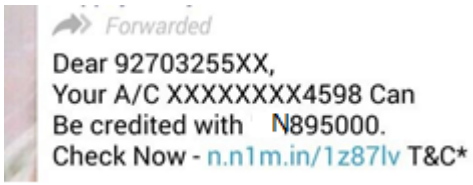


Fig. 6. *Spear Phishing example*

Phone Phishing

Phone phishing encompasses fraudulent messages that appear to originate from banks or network operators. Victims may receive SMS notifications claiming that their SIM card has expired, urgent updates to their bank details are required, or a new service has been activated on their device (Ibrahim et al., 2020). These messages often prompt the recipient to access a specific webpage, thereby exposing them to potential attacks.

Fig. 7. *Phone Phishing example*

Pharming (Domain Name Server-based Phishing)

Another form of phishing is pharming, which involves the manipulation of domain name servers to redirect victims to fraudulent websites. This can result in data or financial loss for the victim (Ibrahim et al., 2020).

Search engine indexing phishing

Search engine indexing phishing is another type of phishing that involves the use of attractive advertisements and offers to mislead victims with broken links or IP addresses.

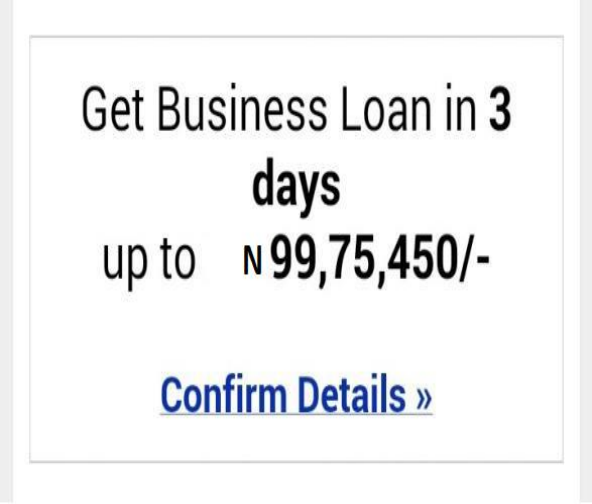


Fig.8. *Search engine indexing phishing*

Games, Social Networks, and Prizes

Games elements on certain websites encourage users to play particular games, ssimilar to "wheel games" or "three questions games" (Eze et al., 2018).

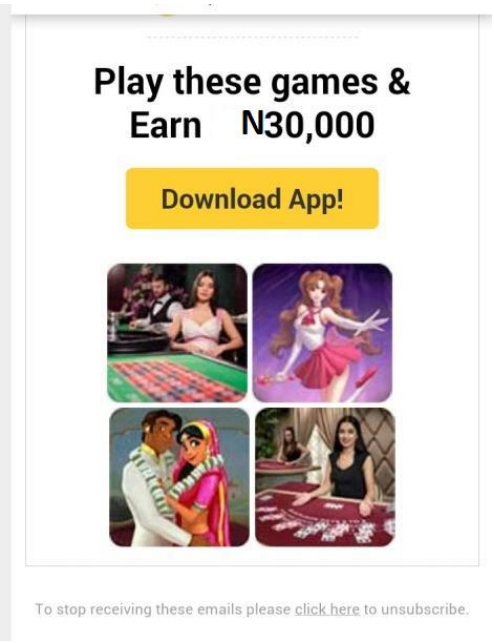


Fig.9. *Example of games, Social Networks, and Prizes*

Impersonation by creating a fake user

Creating fake users and using them as a way to make offers look genuine and gain the victim's trust is another way to carry out phishing attacks. These fake user accounts are essentially JavaScript code embedded as plugins on these phishing sites (Luminita, 2011). They trick victims into believing that someone has won the prize, and then take further steps.

Fig.10. *Fake user*

Sharing and Spreading

When you "earn" these games and rewards, the Website invites you to share more links with your social contacts through various social networks such as WhatsApp, Facebook. This is done to increase the attack's propagation range and increase the size of the target network.

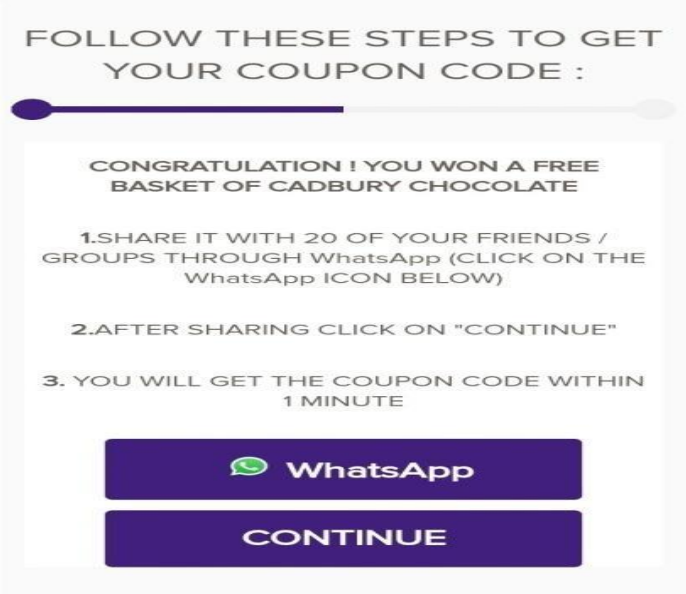


Fig.11. *Sharing and Spreading example*

2.2 RISKS AND THREATS ASSOCIATED WITH E-LEARNING SYSTEMS

This section provides an overview of the main cybersecurity risks associated with online systems and distributed e-learning systems. Important participants in the e-learning system are (Li et al., 2020):

Writer

As you know, writers can provide access to books and journal articles to a wide range of students. you can evolve to iimplement the content of these documents. Only registered students have access to these lecture notes, term papers and exam papers, so it is the writer's duty to protect the data from unauthorized use, alteration and reuse in various e-learning related situations.

Educators

Discussions are an important part of each course lesson. One form of discussion is an online forum. An advantage of online forum discussions over oral discussions is that all documents are stored electronically on a server. However, storing discussion, digitally poses a significant risk to the privacy of students and educators, but in any educational system, maximal interaction helps clarify understanding for both students and educators. In the long run, only robust security mechanisms can trigger this kind of interaction. In the examination system, the examination questions and questionnaires are standardized, and the academic freedom of individual faculty members may be restricted, and the risk of the examination is directly linked to misconduct. Additionally, educators should be concerned about assessment availability and non-repudiation prevention, and the risk of students receiving unaltered questionnaires.

Entry

All entry must be aware of all documents they receive from the Institute, educators, or other students. Because if an intruder has processed a questionnaire or other important documents, it must be considered that a problem occurred during the inspection. User IDs and passwords, in many attacks, provide an excellent opportunity for attackers to prevent authorized learners from accessing eLearning servers. Phishing tricks learners into entering sensitive information into fake websites that look like genuine e-learning websites.

Administrator

There are many risks associated with e-learning platforms, including fraudulent individuals impersonating students and creating tests on behalf of registered students, or assisting in the creation of online exams without authorization. Legal issues such as copyrights, online tests, and sending official documents can therefore be a big problem for these participants. In this case, the administrator must handle course enrolment and, if necessary, cancellation of enrolment. Enrolling a given student in multiple courses poses a risk to the entire organization. You should have a plan for testing your backup and recovery processes. Otherwise, it will be difficult to create a plan.

2.3 STRATEGIES OF MITIGATION AGAINST PHISHING ATTACKS

To combat phishing attacks effectively, it is essential to incorporate interpretations of terms developed through literature analysis. Anti-phishing systems encompass software and tool-based strategies, including standalone systems, programmatic design approaches, and mitigation tools. Models and frameworks play a crucial role in defending against phishing attacks, encompassing activities to mitigate such attacks and machine learning-based models to enhance anti-phishing capabilities. Additionally, human-centered mitigation strategies focus on improving the ability of individuals to identify and respond to phishing attempts.

By considering these modifiers, a comprehensive solution can be developed to address the challenges and risks associated with e-learning platforms and phishing attacks.

This text provides guidelines and recommendations for enhancing skills related to e-learning security. These include organizing anti-phishing training sessions and conducting assessment quizzes. Additionally, key concepts and techniques that should be considered when developing strategies to mitigate security risks. The study revealed that the main concepts and technologies utilized in mitigation strategies are machine learning, neural networks, deep learning, cryptography, human-centric approaches, and secure e-learning systems (Chiew et al., 2019).

In response to growing threats, researchers have developed a number of measures and solutions to improve e-learning security. This section summarizes relevant discussions in the literature (Chang, 2016). Thanks to new technologies, e-learning has become more user-centric and secure.

Biometrics

Despite the availability of authentication technologies such as passwords, smart cards, digital signatures, and digital certificates, there is still a risk of unauthorized access by malicious individuals. For instance, rogue students may misuse passwords while submitting assignments, participating in surveys, or downloading course materials. Biometric authentication offers an additional layer of security in such scenarios. The advantage of biometric computer authentication lies in its reliance on unique personal characteristics, making it difficult to replicate or steal (Ciangaxatapu et al., 2020).

Digital Rights Management

Digital Rights Management (DRM) is a crucial aspect of managing intellectual property rights in the digital realm. Various stakeholders, such as writers, artists, scholars, for-profit companies, and consumers, have distinct motivations for implementing DRM. Writers and artists seek control over the usage of their creative works, scholars aim to ensure proper attribution, for-profit companies support business models that rely on licenses and fees, and consumers desire a legal and cost-free environment. It is important to note that rights themselves are not inherently technical but are shaped by laws, beliefs, and practices. However, technology plays a pivotal role in facilitating the transmission, verification, interpretation, and enforcement of digital rights (Ibrahim et al., 2020)

Watermarking

One effective solution for implementing DRM is watermarking. This technique allows for the inclusion of hidden copyright notices, as well as audio, video, and image signals within digital content (Chang, 2016). For instance, in the context of e-learning systems, watermarking can safeguard the multimedia database server from unauthorized use. By employing watermarking, certain e-learning information remains invisible to viewers, the risk of hacking is significantly reduced. E-learning platforms typically consist of diverse web-based applications that exhibit high interoperability and share similar authentication models. In a typical scenario, a student accessing an e-learning application is required to provide a "shared secret," such as a password or PIN number, along with their student ID. The password is securely stored in the database through a one-way hash function during registration. During the verification process, the student's submitted password is hashed and compared with the stored hash value. This authentication mechanism ensures the legitimacy of the student.

Distributed Firewall Solution

Software application that protects corporate network servers and end-user computers from unwanted intrusions such as distributed firewalls is considered server-based security. The difference between personal firewalls and distributed firewalls is that the latter have important advantages such as centralized management, logging, and sometimes granular access control (Muutode & Parwe, 2019). These features are necessary for implementing corporate security policies in large organizations.

Encryption

The purpose of confidentiality is to prevent disclosure of information or data to unauthorized individuals or organizations. One of the techniques in this aspect is encryption (Drzani, 2014). Cryptography plays an important role in the design and implementation of almost every kind of electronic system. Various cryptographic tools are required to implement security in Internet-based transactions. Encryption is a technology of data transformation Applications in inconsistent, encrypted, or unintelligible formats. This includes research into mathematical algorithms related to information security such as data integrity and authentication. Symmetric key cryptography and asymmetric key cryptography are two other important encryption types.

Tab.2. *Suggested policies based on preventative and detection techniques for people and organizations*

Principal Category	***Directives***
Put endpoint security in place.	- Install endpoint protection. - Develop a technique for identifying threats to intelligent networking. Update computers' hardware and software on a regular basis. Use firewalls, email blocks, browser extensions, and the most recent version of antivirus software. Make use of intrusion detection systems for hosts (HIDS). Follow the security instructions provided by the vendor.
Put access restrictions in place.	Put limitations on access in place. Install tripwires for websites. Use administrator authentication that requires several factors, such as Microsoft Multi-Factor Authentication (MFA). Employ email authentication with DMARC. Observe login instructions.
Observe security guidelines	Respect security protocols. Adjust company policy to allow for anti-phishing and targeted security training, especially for individuals who pose a risk to others. Establish reporting protocols.
Preserve efficiency.	- Create and maintain password protection guidelines. - Discuss potential threats, compromise indicators, and internal best practices. - Establish backup plans - Provide privacy-respecting data processing and sharing. - Provide a Standard Solution (SS) that would enable an experienced writer to draft several sets of guidelines and then utilize them again.
Put device policies into action.	- Establish and set aside money for life-cycle management so that aging equipment can be retired and not easily replaced. - To maintain an up-to-date list of all allowed and illegal devices on the network. Create a policy in collaboration with internal and external manufacturing stakeholders to enable timely updates. - Develop a patching plan to minimize equipment failures. Before buying, take into account how long you think the devices will last.
Remember the guidance.	Verify every call that is received for the authority. - Refrain from sharing information unless you expected to

> hear from the other person.
> - Employ cybersecurity specialists.

Given the dynamic nature of attackers and the possible sensitivity of data, a key issue for future exploration will be the difficulty in giving comparable evaluations among various phishing detection algorithms due to the lack of established benchmarks and reference datasets (Ozcan et al., 2023).

3.0 RESULTS AND DISCUSSION

The discussion revolved around the techniques employed by attackers to carry out phishing attacks, wherein a third party covertly intercepts data exchanged between parties and gains unauthorized access to valuable information within e-learning systems. The risks and threats associated with key participants in the e-learning system were also examined, along with strategies to safeguard data from unauthorized use, alteration, and reuse in diverse e-learning scenarios. Additionally, mitigation measures against phishing attacks, particularly those relying on software and tools, were explored. These measures encompassed stand-alone systems, programmatically designed methods, and tools aimed at mitigating the impact of such attacks.

Numerous researchers have endeavoured to develop different approaches for detecting and protecting against phishing attacks, yet these efforts have often resulted in significant losses. Systematic literature reviews (SLRs) were conducted to assess the effectiveness of various countermeasures against phishing attempts, given the gravity of the situation.

The research on phishing has witnessed a notable surge, particularly in terms of the methods employed by attackers and the domains they target (Bhavsar et al., 2018). According to Table 1 and Figure 2 of a comprehensive online study conducted between 2020 and 2022, phishing attacks were most prevalent in areas such as payments, webmail, and finance. This observation suggests a consistent increase in the frequency of phishing attacks each year, with certain areas exhibiting a heightened vulnerability and concentration of attacks.

4.0 CONCLUSION

Phishing attacks can be launched through various means. However, this study primarily focuses on the detection and prevention techniques applicable to e-learning environments, aiming to empower clients and learners to take necessary precautions against such attacks in the future. The work presented here encompasses an exploration of different types of attacks, along with their prevention and detection mechanisms.

We provide a brief overview of the extensive utilization of email and digital media, highlighting their susceptibility to cybercrime when used without caution. Furthermore, we delve into the various techniques employed in phishing, focusing solely on the phishing process. This document presents an outline of well-known phishing scams. Additionally, we present measures that can aid in the identification of phishing attacks and safeguard individuals from falling victim to such malicious activities. Phishing stands as one of the most prevalent and rapidly expanding forms of cybercrime. Failure to exercise proper precautions and care when engaging in digital and electronic communication can result in significant financial and data losses. Given the ever-evolving nature of phishing assaults, there is an urgent need for effective strategies to mitigate these attacks, which is a major problem for further research and the difficulty in providing comparable evaluations among different phishing detection algorithms due to the lack of established benchmarks and reference datasets, given the dynamic nature of attackers and the potential sensitivity of data. Lastly, the target audience for this paper includes but not limited to academics and business professionals as well as anybody with an interest in cyber security. To assist researchers in organizing their next steps, it offers existing solutions, and current trends. Apart from offering guidelines and recommendations that are specifically crafted with the organization's viewpoint in mind, it provides industry practitioners with an up-to-date summary of the most recent research on phishing attacks and could prove beneficial to incorporate in their respective environments. This paper presents the state of the art in mitigation strategies and highlights current phishing trends for a general audience interested in cyber security.

DECLARATION OF COMPETING INTEREST

The authors affirm that they possess no known competing financial interests or personal relationships that could have potentially influenced the findings presented in this paper.

REFERENCES

Abdillah, R., Shukur, Z., Mohd, M., & Murah, M. Z. (2022). Phishing classification techniques: A systematic literature review. *IEEE Access*, 10, 41574-41591.

Alaubaci, F. S., Almazros, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. *IEEE Access*, 12, 8373-8389. https://doi.org/10.1109/access.2024.3351946

Altaher, A. (2021). Intelligent ensemble learning approach for phishing website detection based on weighted soft voting. *Mathematics*, 9(21), 2799. https://doi.org/10.3390/math9212799

Apandi, S. H., Sallim, J., & Sidek, R. M. (2020). Types of anti-phishing solutions for phishing attacks. IOP Conference Series: *Materials Science and Engineering*, 769, 012072.

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. W. (2021). A systematic literature review on phishing and anti-phishing techniques. arXiv. https://doi.org/10.48550/arXiv.2104.01255

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, 182(33), 27-29. https://doi.org/10.5120/ijca2018918266

Catal, C., Giray, G., Iskinenlagan, B., Kumar, S., & Shukla. (2022). Applications of deep learning for phishing detection: A systematic literature review. *Knowledge and Information Systems*, 64(6), 1457-1500. https://doi.org/10.1007/s10115-022-01672-

Chang, V. (2016). Review and discussion: E-learning for academia and industry. *International Journal of Information Management*, 36(3), 476-485. https://doi.org/10.1016/j.infomgt.2015.12.007

Chanti, S., & Chithralekha, T. (2019). Classification of anti-phishing solutions. *SN Computer Science*, 1(1). https://doi.org/10.1007/s42979-019-0011-2

Chen, S., Lu, Y.-X., & Lim, D. J. (2022). Phishing target identification based on neural networks using category features and images. *Security and Communication Networks*, 2022, 1-12. https://doi.org/10.1155/2022/5653270

Chiew, K. L., Tan, C. L., Wong, K. S., Yong, K. S. C., & Trong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, 484, 153-166. https://doi.org/10.1016/j.ins.2019.01.064

Ciangaxatapu, T., Jaidhat, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: Review and approaches. *Artificial Intelligence Review*, 53(7), 5019-5081. https://doi.org/10.1007/s10462-020-09814-9

Desolda, G., Ferro, L. S., Marrella, A., Catarsi, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), 1-35. https://doi.org/10.1145/3469886

Das, A. S., Baki, A., El Aassal, & Vetm. (n.d.). Phishing research from the society perspective: A comprehensive re-examination of BEE Common Surveys Tuts. *Journal*, 22(1), 671-704. Available at https://1911.00953

Dima, A., Bugheanu, A. M., Boghian, R., & Madsen, D. O. (2022). Mapping knowledge area analysis in e-learning systems based on cloud computing. *Electronics*, 12(1), 62. https://doi.org/10.3390/electronics12010062

Drzani, M. (2014). Securing e-learning platforms. 2014 International Conference on Web and Open Access to Learning (ICWOAL), *Dubai, United Arab Emirates*, 1-4. https://doi.org/10.1109/ICWOAL.2014.7009237

Eze, S. C., Chinedu-Ere, V. C., & Belle, A. O. (2018). The utilisation of e-learning facilities in the educational delivery system of Nigeria: *A study of M-University. International Journal of Educational Technology in Higher Education*, 15(1). https://doi.org/10.1186/41239-2018-0116-2

Ennu, G., Martes, M., & Boratto, L. (2018). A multi-brometne system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113, 83-92. https://doi.org/10.1016/j.patrec.2017.03.027

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management systems. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. https://doi.org/10.1109/isdfs49300.2020.9116415

Li, T., Kou, G., & Peng, Y. (2020). Improving malicious URLs detection via feature engineering: Linear and nonlinear space transformation methods. *Information Systems*, 91, 101494. https://doi.org/10.1016/j.is.2020.101494

Luminita, D. C. (2011). Information security in e-learning platforms. Procedia - *Social and Behavioral Sciences*, 15, 2689-2693. https://doi.org/10.1016/j.sbspro.2011.04.171

Muutode, A. R., & Parwe, S. S. (2019). An overview on phishing, its types and countermeasures. *International Journal of Engineering Research and Technology*, 8(12). https://doi.org/10.17577/ijertv8is120260

Nadeem, M., Zahra, S., Abbasi, M., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing attack, its detections and prevention techniques. *International Journal of Wireless Information Networks.* https://doi.org/10.37591/gwan

Ozcan, A., Catal, C., Demmez, E., & Senturk, B. (2023). A hybrid DNN-LSTM model for detecting phishing URLs. *Neural Computing & Applications*, 35, 4957-4973. https://doi.org/10.1007/s00521-02

Prosen, M., Kamuž, I., & Ličen, S. (2022). Evaluation of e-learning experience among health and allied health professions students during the COVID-19 pandemic in Slovenia: An instrument development and validation study. *International Journal of Environmental Research and Public Health*, 19(8), 4777. https://doi.org/10.3390/ijerph19084777

Safi, A., & Singh, S. (2013). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, 35(2), 590-611. https://doi.org/10.1016/j.jksuci.2025.01.004

Sallaum, A., Gaber, T., Vaderz, & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10, 65703-65727. https://doi.org/10.1109/access.2022.31830838918286.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 35 – 52 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

პოსტკვანტური ციფრული ხელმოწერა ვერკლის ხისა და ლატისების გამოყენებით

POST-QUANTUM DIGITAL SIGNATURE USING VERKLE TREES AND LATTICES

Maksim Iavich[1], Tamari Kuchukhidze[1], Avtandil Gagnidze[2]

[1] Department of Computer Science, Caucasus University, 0102, Georgia
[2] East West University, 9 Vakhtang Gorgasali St, Tbilisi

რეზიუმე: ბოლო წლებში კვანტურ კომპიუტერებზე კვლევები მნიშვნელოვნად განვითარდა. თუკი კაცობრიობა ოდესმე შექმნის ეფექტურ კვანტურ კომპიუტერს, არსებული საჯარო გასაღების უმეტესი კრიპტოსისტემებს პრობლემები შეექმნება. ასეთი სახის კრიპტოსისტემები დღსდღეობით გვხვდება ბევრ კომერციულ პროდუქტში. ჩვენ შევიმუშავეთ შედეგები, რომლებიც, ერთი შეხედვით გვიცავს კვანტური შეტევებისგან, მაგრამ ისინი სახიფათო და არაეფექტურია ყოველდღიურ ცხოვრებაში გამოსაყენებლად. ნაშრომში გაანალიზებულია ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის მეთოდები. შეფასებულია მერკლის ხეზე დაფუძნებული ელექტრონული ხელმოწერა. ვერკლის ხის და ვექტორული ვალდებულებების გამოყენებით ნაშრომი იკვლევს ახალ იდეებს.
ამ სტატიაში წარმოვადგენთ უნიკალურ ტექნოლოგიას, პოსტკვანტური ციფრული ხელმოწერის სისტემის შემუშავებისთვის, რომლისთვისაც ვიყენებთ უახლეს ვერკლის ხეს. ამ მიზნისთვის გამოიყენება ვერკლის ხე, ვექტორული ვალდებულებები და ისეთი ვექტორული ვალდებულებები, რომლებიც დაფუძნებულია ლატისებზე, პოსტკვანტური თვისებებისთვის. ნაშრომში ასევე მოცემული პოსტკვანტური ხელმოწერის დიზაინის ცნებები ვერკლის ხის გამოყენებით.

საკვანძო სიტყვები: პოსტ-კვანტური კრიპტოგრაფია; კვანტური კრიპტოგრაფია; გვერდითი არხის თავდასხმები; CRYSTALS-Kyber; მასკირება; ღრმა სწავლება; ლატისებზე დაფუძნებული კრიპტოგრაფია.

ABSTRACT: Significant advancements have been achieved in the field of quantum computing in recent years. If somebody ever create a sufficiently strong quantum computer, many of the public key cryptosystems in use today might be compromised. Kyber is a post-quantum encryption technique that depends on lattice problem hardness, and it was recently standardized. Despite extensive testing by the National Institute of Standards and Technology (NIST), new investigations have demonstrated the effectiveness of Crystals-kyber attacks and their applicability in non-controlled environments.
We investigated CRYSTALS-Kyber's susceptibility to side-channel attacks. In the reference implementation of Kyber512, additional functions can be compromised by employing the selected ciphertext. The implementation of the selected ciphertext allows the attacks to succeed. Real-time recovery of the entire secret key is possible for all assaults.

KEYWORDS: post-quantum cryptography; quantum cryptography; side-channel attacks; CRYSTALS-Kyber; masking; deep-learning; lattice-based cryptography.

1. შესავალი

კვანტური გამოთვლები საბოლოოდ უფრო გავრცელებული გახდება, რაც გამოიწვევს პოსტკვანტური კრიპტოგრაფიის განვითარებას. პოსტკვანტური კრიპტოგრაფია, რომელიც ასევე ცნობილია როგორც კვანტური დაშიფვრა, არის კლასიკური კომპიუტერების დაცვის საშუალება კვანტური კომპიუტერის შეტევებისგან [1]. კვანტურ კომპიუტერებს შეუძლიათ რთული გამოთვლების შესრულება ბევრად უფრო სწრაფად, ვიდრე ჩვეულებრივ დესკტოპ კომპიუტერებს, რასაც შეიძლება წლები დასჭირდეს ჩვეულებრივი კომპიუტერებისთვის. კვანტურმა კომპიუტერმა შეიძლება დაარღვიოს სტანდარტული კრიპტო სისტემების უმეტესობა, თუ არა ყველა, რომელიც ამჟამად ვიყენებთ პრაქტიკაში.

კვანტური გამოთვლის განვითარებისას, უფრო საგულისხმო ხდება კრიპტოგრაფიის მიმდინარე მეთოდების ეფექტურობა. იგულისხმება გავრცელებული მეთოდები, როგორიცაა RSA ან ელიფსური მრუდის კრიპტოგრაფია (ECC). RSA-ს უსაფრთხოება ეყრდნობა რთულ მათემატიკურ ამოცანებს, როგორიცაა მთელი რიცხვების ფაქტორიზაცია. კვანტურ გამოთვლას, შორის ალგორითმის მსგავსი ტექნიკის გამოყენებით, შეუძლია ამ პრობლემების გადაჭრა, რაც მნიშვნელოვან საფრთხეს უქმნის RSA-ს [2], შესაბამისად ყველა სისტემას რომლებიც RSA–ზე არის დაფუძნებული. ეს არის ერთ–ერთი მაგალითი არსებული მეთოდების არაეფექტურობის.

კვანტური გამოთვლების ზრდა გვიჩვენებს, რომ დაშიფვრის ტრადიციული მეთოდები შეიძლება მოძველდეს. ამან განაპირობა მონაცემთა დაცვის ახალი მეთოდების შემუშავება, როგორიცაა ლატისებზე დაფუძნებული დაშიფვრა, რომელიც შექმნილია კვანტური კომპიუტერის შეტევების წინააღმდეგობის გასაწევად [3].

ამ სირთულის გაცნობიერებით, პოსტ-კვანტური კრიპტოსისტემები, რომლებსაც შეუძლიათ უსაფრთხოდ და წარმატებით გაუძლონ კვანტურ შეტევებს, უნდა განვავითაროთ და გამოვიყენოთ [4–5]. კვანტური გამოთვლების სრულყოფის შემთხვევაში, ჩვეულებრივი ასიმეტრიული მეთოდები, როგორიცაა RSA, ვერ იქნება ადეკვატური პირადი მონაცემების დასაცავად. კვანტური ტექნოლოგიების განვითარების შედეგად აუცილებელი გახდა მუდმივად შევქმნათ და განვავითაროთ მოქნილი პოსტკვანტური სისტემები [6].

არსებული კვანტური კომპიუტერული საფრთხის მოსაგვარებლად, სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST)–მა 2016 წელს დაიწყო პოსტ-კვანტური კრიპტოგრაფიის სტანდარტიზაციის ინიციატივა (NIST PQC). მისი მიზანია შეიქმნას ძლიერი კრიპტოგრაფიული სტანდარტები, რომლებიც შეძლებენ წინააღმდეგობა გაუწიონ კვანტურ კომპიუტერულ შეტევებს და უზრუნველყონ მგრძნობიარე მონაცემები.

NIST–მა ეს პროცესი დაიწყო კრიპტოგრაფიის საზოგადოების მიერ წარმოდგენილი პოტენციური ალგორითმების ჯგუფების შერჩევით. ეს ალგორითმები ფართოდ გამოიცადა კვანტური შეტევების მიმართ, როგორი გაუძლებდნენ. ბოლო სტადიებში გადავიდა

ალგორითმები, რომლებიც ეფუძნება რთულ მათემატიკურ ამოცანებს, როგორიცაა წრფივი შეცდომის გამოსწორების კოდის დეკოდირება (linear error-correcting code decoding) და ლატისები, რომელთა გადაჭრა ძნელია კვანტური კომპიუტერებისთვის.

2022 წლის ივლისში NIST-მა 2022 გამოაცხადა, რომ CRYSTALS-Kyber გახდება ახალი სტანდარტი გასაღების პარამეტრების და საჯარო გასაღების დაშიფვრისთვის (PKE) [7]. ეს არის მთავარი. ამ არჩევანის მიზეზი არის ის, რომ იგი იდენტიფიცირებულია, როგორც ძირითადი ინკაფსულაციის მექანიზმი (KEM), რომელიც უზრუნველყოფს IND-CCA2 შემთხვევით ორაკულების მოდელებში, რომლებიც არის როგორც კლასიკური, ასევე კვანტური. შეცდომებით სწავლის მოდულის სირთულე (M-LWE), რომელიც ხაზს უსვამს უცნობ ხმაურს, ქმნის CRYSTALS-Kyber-ის უსაფრთხოების საფუძველს. გარდა ამისა, CRYSTALS-Kyber სწრაფად ჩართეს ეროვნული უსაფრთხოების სააგენტოს (NSA) მიერ ეროვნული უსაფრთხოების აპლიკაციებისთვის შემოთავაზებული კრიპტოგრაფიული ალგორითმების კოლექციაში [8]. ეს ხაზს უსვამს ალგორითმის მნიშვნელობას კრიპტოგრაფიული სისტემების დაცვაში ახალი კვანტური საფრთხეებისგან.

ცნობილია თავისი IND-CCA2 უსაფრთხოებით, მისი გამოვლენა შეუძლებელია ადაპტური შერჩეული შიფრული ტექსტის შეტევის დროს [9]. იმის გამო, რომ ის შეიცავს უცნობი ხმაურის ჩასმას წრფივ განტოლებებში, მოდულის სწავლა შეცდომებით (M-LWE) პრობლემა რთულია, რაც განსაზღვრავს/უზრუნველყოფს მის უსაფრთხოებას.

CRYSTALS-Kyber და სხვა პოსტკვანტური დაშიფვრის ალგორითმების ცნობილი სისუსტეებია დაცულ პროგრამული უზრუნველყოფის დანერგვაში. გვერდითი არხის ანალიზის მოწინავე მეთოდებმა, განსაკუთრებით ღრმა სწავლის გამოყენებით, შეძლეს ამ განხორციელებების დარღვევა. ამ მოწყვლადობამ განაპირობა უკეთესი დაცვის განვითარება და CRYSTALS-Kyber-ის გაუმჯობესებული დანერგვა.

მნიშვნელოვანია შევაფასოთ რამდენად კარგად ეწინააღმდეგება CRYSTALS-Kyber-ის დანერგვა გვერდითი არხის თავდასხმებს. ეს შეტევები იყენებს არაპირდაპირ, დაკვირვებადი არხების ინფორმაციას, როგორიცაა დრო ან ელექტროენერგიის მოხმარება და სერიოზულ საფრთხეს უქმნის კრიპტოგრაფიულ უსაფრთხოებას.

Kocher et al. [10] მიაღწია მნიშვნელოვან წინსვლას ამ სფეროში დიფერენციალური გვერდითი არხის ანალიზის შემუშავებით, რომელიც იყენებდა ფიზიკურ მონაცემებში განსხვავებებს. ღრმა სწავლაზე დაფუძნებული გვერდითი არხის ანალიზი [11] იყო კიდევ ერთი მნიშვნელოვანი განვითარება, რამაც შესაძლებლობა მოგვცა თავდასხმების განხორციელება მომხდარიყო სხვადასხვა კრიპტოგრაფიულ სისტემაზე. ტრადიციული თავდაცვა ვერ უძლებს ამ თავდასხმებს. არანაკლებ მნიშვნელოვანია, Wang et al.-ის [12] შეცდომის ინექციის მეთოდი, რომელიც არღვევს რთულ სამიზნეებს, როგორიცაა CRYSTALS-Kyber-ის ტექნიკის დანერგვა არადიფერენციალური თავდასხმების დიფერენციალურზე გარდაქმნით.

ბევრი საპირისპირო ღონისძიება, კონტრზომა არსებობს, მათ შორის, დაფარვა/მასკირება [13-15], არევა [16-18], რანდომიზებული საათი [19-20], შემთხვევითი შეფერხებების ჩასმა [21-23], მუდმივი წონის დაშიფვრა [24] და კოდის პოლიმორფიზმი [25- 26], გამოიყენება გვერდითი

არხის თავდასხმების შესამცირებლად. ინფორმაციის გაჟონვის თავიდან ასაცილებლად ფიზიკურად რაოდენობრივი არხებით, როგორიცაა დრო [27–28], ენერგიის მოხმარება [29–30] ან ელექტრომაგნიტური გამოსხივება [31–32], ეს კონტრზომები კრიპტოგრაფიული სისტემების დაცვას ცდილობს.

საბოლოოდ, გვერდითი არხის თავდასხმები (side-channel attacks) უფრო დახვეწილი ხდება, რაც ხაზს უსვამს კრიპტოგრაფიული განხორციელების უსაფრთხოების მუდმივი შეფასების და გაუმჯობესების მნიშვნელობას - განსაკუთრებით მაშინ, როდესაც საქმე ეხება პოსტკვანტურ კრიპტოგრაფიის ალგორითმებს, როგორიცაა CRYSTALS-Kyber.

2. კიბერის და CRYSTALS-კიბერის მიმოხილვა

კიბერი (Kyber) არის უსაფრთხო გასაღების ინკაფსულაციის მექანიზმი (KEM), რომელიც დაფუძნებულია შეცდომებთან სწავლის (LWE) პრობლემაზე, რომელიც იყენებს ლატისების მოდულს. ეს არის NIST–ის პოსტ-კვანტური კრიპტოგრაფიის პროექტის ერთ-ერთი კანდიდატი. წინადადებაში შედის სამი პარამეტრის ნაკრები, უსაფრთხოების სხვადასხვა დონისთვის: Kyber-512 (მსგავსი AES-128–ის), Kyber-768 (მსგავსი AES-192–ის) და Kyber-1024 (მსგავსი AES-256–ის).

რეკომენდებულია კიბერის გამოყენება ჰიბრიდულ რეჟიმში, მისი ინტეგრირება უსაფრთხოების ცნობილ „წინასწარ კვანტურ“ პროცედურებთან. დიფი-ჰელმანის გაერთიანება ელიფსურ მრუდთან არის ერთი–ერთი კონკრეტული მაგალითი. ეს მეთოდი იყენებს როგორც პოსტკვანტური, ასევე კლასიკური კრიპტოგრაფიის უპირატესობებს [33].

მიზანშეწონილია გამოვიყენოთ Kyber-768 პარამეტრის ნაკრები. ეს პარამეტრის შერჩევა გვთავაზობს 128 ბიტზე მეტ უსაფრთხოებას ყველა ცნობილი ჩვეულებრივი თუ კვანტური შეტევის წინააღმდეგ. ეს მიღებულია კონსერვატიული ანალიზის მიხედვით, რომელმაც მიიღო ეს გადაწყვეტილება. კრიპტოგრაფიის სამყაროში, 128 ბიტიანი უსაფრთხოება განიხილება, როგორც უკიდურესად ძლიერი და მდგრადი, როგორც ცნობილი, ისე უცნობი საფრთხეების მიმართ.

2022 წლის ზაფხულში, NIST-მა (აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა) სტანდარტიზაციისთვის შეარჩია CRYSTALS-Kyber, კვანტურად უსაფრთხო გასაღების კაფსულაციის ახალი მეთოდი. CRYSTALS ნიშნავს კრიპტოგრაფიულ კომპლექტს ალგებრული ლატისებისთვის.

Kyber არის CCA-უსაფრთხო KEM სქემა, რომელიც არის CRYSTALS-Kyber-ის ნაწილი. შერჩეული ღია ტექსტის თავდასხმის (CPA) უსაფრთხო PKE ტექნიკაზე დაშენებულია კიბერი, აგებულია CCAKEM.CPAPKE (სურათები 1 და 2), სადაც გამოვიყენებთ Fujisaki-Okamoto (FO) ტრანსფორმაციის მორგებული ვერსიას [34].

CPAPKE.KeyGen()

seed $_A \leftarrow \mathcal{U}(\{0,1\}^{256})$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$e \leftarrow \mathcal{B}_{\eta_1}\left(R_q^{k\times 1}\right)$
$b = As + e_{p_1}$
$pk = (seed_A, b), sk = s$
return (pk, sk)

CPAPKE. Enc$(pk = (seed_A, b), m, r)$

$A \leftarrow \mathcal{U}\left(R_q^{k\times k}; seed_A\right)$
$s' \leftarrow \mathcal{B}_{\eta_1}\left(R_\eta^{k\times 1}; r\right)$
$e' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{k\times 1}; r\right)$
$e'' \leftarrow \mathcal{B}_{\eta_2}\left(R_q^{1\times 1}; r\right)$
$u = \lfloor (As' + e') \cdot 2^{d_u}/q \rceil$
$v = [(b \cdot s' + e'' + encode(m)) \cdot 2^{d_v}/q]$
return $c = (u, v)$

CPAPKE.Dec(s, $c = (u, v)$)

$y = \lfloor v \cdot q/2^{d_v} \rceil - s\lfloor u \cdot q/2^{d_u} \rceil$
$m' = decode(y)$
return m'

ფიგურა 1. CCAPKE ალგორითმები

Kyber.KeyGen()

$z \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(pk, \mathrm{s}) = \mathrm{CPAPKE.KeyGen()}$

$sk = (\mathrm{s}, pk, \mathcal{H}(pk), z)$

return (pk, sk)

Kyber.Encaps (pk)

$m \leftarrow \mathcal{U}(\{0,1\}^{256})$

$(\hat{K}, r) = \mathcal{G}(m, \mathcal{H}(pk))$

$c = \mathrm{CPAPKE.\,Enc}(pk, m, r)$

$K = \mathrm{KDF}(\hat{K}, \mathcal{H}(c))$

return (c, K)

Kyber.Decaps $(sk = (\mathrm{s}, pk, \mathcal{H}(pk), z), c)$

$m' = \mathrm{CPAPKE.Dec(s,}\ c)$

$(\hat{K}', r') = \mathcal{G}(m', \mathcal{H}(pk))$
$d' = \mathrm{CPAPKE.Enc}\ (pk, m', r')$
if $c = c'$ then

return $K = \mathrm{KDF}(\hat{K}, \mathcal{H}(c))$

else

return $K = \mathrm{KDF}\left(z, \mathcal{H}(c)\right)$

end if

ფიგურა 2. CCAPKE ალგორითმები

CRYSTALS-Kyber იყენებს რგოლის (ring) ელემენტების ვექტორებს R_q^k-ში, სადაც k არის მოდულის რანგი, რომელიც გამოიყენება უსაფრთხოების დონის გასაზომად. CRYSTALS–Kyber-ის შემთხვევაში გვაქვს სამი განსხვავებული ვარიანტი k=2, 3 და 4-ისთვის, Kyber-512, Kyber-768 და Kyber-1024. ვინაიდან მისაღები იმპლემენტაცია მხარს უჭერს Kyber-512-ს, ეს ვერსია არის მთავარი აქცენტი. რიცხვთა თეორიული ტრანსფორმაცია (NTT) გამოიყენება CRYSTALS-Kyber-ის მიერ R_q-ში გამრავლების ეფექტურად შესასრულებლად.

მნიშვნელობა K იქმნება შეტყობინებისა და საჯარო გასაღების ჰეშის კომბინაციით, CPAPKE.Enc ფუნქციის გამომავალი ჰეშთან, გასაღების გენერაციის ფუნქციის გამოყენებით. ეს ნიშნავს, რომ დაშიფვრის გასაღები (K) მომდინარეობს შეტყობინების, საჯარო გასაღებისა და დაშიფვრის ფუნქციის (CPAPKE.Enc) დამატებითი მონაცემებიდან. ეს პროცესი აღწერილია Kyber.Encaps ფუნქციაში, სადაც K იქმნება დაშიფვრის დროს და ხდება მისი დაბრუნება. გაშიფვრის შემდეგ (Kyber.Decaps), K შეიძლება იყოს იგივე, რაც დაშიფვრის დროს ან იქნება ყალბი მნიშვნელობა, რაც დამოკიდებულია დაშიფრული ტექსტის მთლიანობაზე. შემავალი მნიშვნელობა r, რომელიც არის CPAPKE.Enc-ისთვის, მიღებულია შეტყობინებისა და საჯარო გასაღების ჰეშირებიდან, ვიდრე თვითნებური მნიშვნელობის გამოყენებით, უსაფრთხოების გასაძლიერებლად.

შეცდომებზე დაფუძნებული სწავლის სქემებს (Error-Based Learning schemes), როგორიცაა კიბერი, შეიძლება ჰქონდეს გაშიფვრის წარუმატებლობები, რაც თავდამსხმელებმა შესაძლოა გამოიყენონ პირადი ინფორმაციის აღმოსაჩენად. ეს წარუმატებლობა უფრო სავარაუდოა, თუ თავდამსხმელები ქმნიან საიდუმლო ვექტორებს და შეცდომის მნიშვნელობებს CPAPKE.Enc-ში დაშვებული ლიმიტებს მიღმა.

Kyber.Encaps და Kyber.Decaps იყენებენ შეცვლილ Fujisaki-Okamoto-ს ტრანსფორმაციას, რათა უზრუნველყონ შემთხვევითი საიდუმლოების და შეცდომის მნიშვნელობები დაგენერირდეს სწორად და კარგად იყოს დამოწმებული გაშიფვრის დროს.

CRYSTALS-Kyber ალგორითმი იყენებს Fujisaki-Okamoto (FO) ტრანსფორმაციას CCA2 უსაფრთხოების უზრუნველსაყოფად. პირველ რიგში ის დაშიფრულ ტექსტის დეშიფრაციას ახდენს CPA-ის გამოყენებით. შემდეგ ის „ხელახლა დაშიფრავს“ შეტყობინებას ახალი დაშიფრული ტექსტის c' მისაღებად. ამოწმებს, შეესაბამება თუ არა c' თავდაპირველ დაშიფრულ ტექსტს c–ს. თუ ისინი ემთხვევა, შედეგი არის სწორი (True); წინააღმდეგ შემთხვევაში, შედეგი მცდარია (False). სესიის გასაღების K წარმოქმნა დამოკიდებულია ამ შედეგზე. FO ტრანსფორმაცია ხელს გვიწყობს აღმოვაჩინოთ თავდამსხმელის მიერ განხორციელებული ნებისმიერი ცვლილება.

არსებითად ეს კიბერ მექანიზმი გვიცავს თავდამსხმელებისგან, რომლებიც იყენებენ სისუსტეებს დაშიფვრისა და გაშიფვრის პროცესებში. ის განიხილავს პოტენციურ საკითხებს, რომლებიც დაკავშირებულია გაშიფვრის წარუმატებლებთან შეცდომებთან სწავლების სქემებში.

3. გვერდითი არხის თავდასხმები

კრიპტოგრაფიული სისტემები შეიძლება უსაფრთხოდ გამოიყურებოდეს მათემატიკური შეტევებისგან, მაგრამ მაინც არ არიან დაცული გვერდითი არხის თავდასხმებისგან. ამ სტილის შეტევები იყენებენ სისტემების მუშაობის დროს განმავლობაში გაჟონულ მონაცემებს, როგორიცაა ელექტრომაგნიტური გამოსხივება, ხმის ტალღები, ენერგიის მოხმარება ან შესრულების დრო [35]. პირველად გამოვლინდა პოლ კოჩერის მიერ 1996 წელს, გვერდითი არხის თავდასხმები განსაკუთრებით სარისკოა ჩაშენებული სისტემებისთვის. მიუხედავად იმისა, რომ პოსტ-კვანტური კრიპტოგრაფიის (PQC) ბევრი კანდიდატი წინააღმდეგობას უწევს მარტივ დროით შეტევებს, სხვა გვერდითი არხის შეტევების მეთოდებს, როგორიცაა სიმძლავრე და ელექტრომაგნიტური ანალიზი, კვლავ შეუძლიათ საფრთხე შეუქმნან სისტემებს. მკვლევარები მუშაობენ ამ მოწყვლადობის იდენტიფიცირებასა და შერბილებაზე. NIST ხაზს უსვამს გვერდითი არხის თავდასხმებზე წინააღმდეგობის მნიშვნელობას PQC დანერგვაში, რომ ვუზრუნველყოთ ჩვენი სისტემების უსაფრთხოება.

მეცნიერებმა ჩაატარეს საფუძვლიანი გამოკვლევა იმის შესახებ, თუ რამდენად მგრძნობიარეა ლატისებზე დაფუძნებული გასაღების ინკაფსულაციის მექანიზმები (KEM) სხვადასხვა გვერდითი არხის შეტევების მიმართ. მკვლევარებმა ყურადღება გაამახვილეს გვერდითი არხის დახმარებით შერჩეულ დაშიფრული ტექსტის შეტევებზე (CCA), რომლებიც მიზნად ისახავს საიდუმლო გასაღების მოპოვებას ლატისებზე დაფუძნებული გასაღების ინკაფსულაციის მექანიზმებში (KEM) [36-37]. ეს შეტევები მიზნად ისახავს სხვადასხვა პროცესებს, როგორიცაა Fujisaki-Okamoto (FO) ტრანსფორმაცია, შეტყობინების კოდირება/გაშიფვრა, ინვერსიული რიცხვის თეორიული ტრანსფორმაცია (NTT) და შეცდომების გამოსწორების კოდები. გვერდითი არხის თავდასხმები იყენებს არაპირდაპირ არხებს, როგორიცაა დრო ან ენერგიის მოხმარება. კრიპტოგრაფიული ოპერაციების დროს ელექტრო სიგნალებში დაუცველობის დასადგენად, მკვლევარებმა გამოიყენეს ვერტიკალური გვერდითი არხის გაჟონვის გამოვლენა CRYSTALS-Kyber-ის გაშიფვრის პროცესის გასაანალიზებლად.

KYBER-512-ს აქვს ხარვეზები, რომლებიც თავდამსხმელს საშუალებას აძლევს აღადგინოს გასაღები რამდენიმე მარტივი მოთხოვნით, თუკი შემტევმა იცის გაშიფრული შეტყობინებები [38]. ეს შეტევები ფოკუსირებულია შეტყობინების დაშიფვრაზე და ინვერსიულ რიცხვთა თეორიულ ტრანსფორმაციაზე (NTT) სუფთა და m4 სქემებში. m4 სქემა არის Kyber-ის ოპტიმიზებული ვერსია ARM Cortex-M4 CPU-სთვის, რომელიც შედის pqm4 ბიბლიოთეკაში. საიდუმლო გასაღების აღდგენა შესაძლებელია მხოლოდ ოთხი ძიებით თუ საქმე გვაქვს სუფთა სქემასთან და რვა ძიებით შეგვიძლია აღვადგინოთ m4 სქემის შემთხვევაში.

ასევე გვაქვს შეტყობინებების აღდგენის მეთოდები, როგორიცაა შეტყობინებების ციკლური როტაცია და მიზნობრივი ბიტის შებრუნება [39]. ეს მეთოდები მოითხოვს (w + 1) ნაკვალევს (traces) გვერდითი არხის ჰემინგის წონის კლასიფიკატორით. საწინააღმდეგო ზომებით მასკირებისა და არევის/შერწყმის მიუხედავად, აპლიკაციები შესაძლოა მაინც დაუცველი

იყოს. თუმცა, ამ კონტრზომებით დაცულ იმპლემენტაციებზე თავდასხმა მოითხოვს, რომ თავდამსხმელმა შეძლოს მათი დეაქტივაცია შაბლონების შესაქმნელად.

გარდა ამისა, მკვლევარებმა შემოგვთავაზეს აღდგენილ შეტყობინებებზე დაფუძნებული გასაღების აღდგენის შეტევა, რომელსაც დასჭირდება ექვსი კონკრეტული დაშიფრული ტექსტი. მნიშვნელოვანია გვახსოვდეს, რომ KYBER-512 ხმაურის მნიშვნელობა გაიზარდა და CRYSTALS-კიბერის სპეციფიკაცია შეიცვალა, რაც მიუთითებს იმაზე, რომ ახლა საჭიროა უფრო ფრთხილად მომზადებული დაშიფრული ტექსტები [40].

4. მასკირება

მასკირების გამოყენებით ვცდილობთ CRYSTALS-Kyber დავიცვათ გვერდითი არხის თავდასხმებისგან. კრიპტოგრაფიული ალგორითმების არითმეტიკული ქცევის დამალვის მიზნით, საპირისპირო ღონისძიება, რომელიც ცნობილია როგორც მასკირება/შენიღბვა მოიცავს საიდუმლოების დაყოფას ბევრ, ნაწილობრივ რანდომიზებულ აქციებად (სადაც მეხუთე რიგი ეხება საიდუმლო გაყოფას ხუთჯერ). ჩვენ გამოვიყენებთ ტექნიკას სახელწოდებით masking, რათა გავაძლიეროთ CRYSTALS-Kyber გვერდითი არხის შეტევებისგან [41].

სიმძლავრისა და ელექტრომაგნიტური გვერდითი არხის გამოკვლევის ზოგადი დაცვა არის მასკირება. ფუნდამენტურად, მასკირება გულისხმობს ფარული მნიშვნელობის დაყოფას რამდენიმე ნაწილად შემთხვევით. ალგორითმი თითოეულ ეტაპზე დამოუკიდებლად ამუშავებს ამ დაყოფილ ინფორმაციას, აერთიანებს შედეგებს საბოლოო სასურველი შედეგის მისაღებად. დაფარვის დომენის შიგნით მუშაობა აჩერებს x ცვლადის მგრძნობიარე ინფორმაციის გაჟონვას, რადგან ის არასოდეს გამოიყენება პირდაპირ. ესე იგი, პირდაპირ ერთიან ინფორმაციას არ ვიყენებთ. ეს მთლიანი იყოფა რამდენიმე ნაწილად. მგრძნობიარე ცვლადი x იყოფა $\omega + 1$ ნაწილად, ეს არის ω - რიგის შენიღბვა. ვიღებთ $x = x_1 \circ x_2 \circ \dots \circ x_{\omega+1}$, ისე რომ $x = x_1 \circ x_2 \circ \dots \circ x_{\omega+1}$. გვაქვს მასკირების ორი: არითმეტიკული და ლოგიკური (Arithmetic and Boolean) ვარიანტი. შენიღბვის ტექნიკიდან გამომდინარე, "∘" შეიძლება წარმოადგენდეს სხვადასხვა ოპერაციებს. მაგალითად, არითმეტიკული მასკირებისას "∘" არის არითმეტიკული დამატება, ხოლო ლოგიკური მასკირების დროს ეს არის XOR.

გამოთვლების შემთხვევაში ვცდილობთ თავიდან ავიცილოთ საწყისი ინფორმაციის x – ის პირდაპირ გამოყენებას. ოპერაციებზე მოქმედებები სრულდება სხვადასხვა ნაწილებზე დამოუკიდებლად, რაც თეორიულად ხელს უშლის x-ის შესახებ გვერდითი არხის საშუალებებით ინფორმაციის გაჟონვას. ყოველ ჯერზე, როდესაც ვყოფთ ინფორმაციას, ის შემთხვევით არის არჩეული. რანდომიზაცია ჩვეულებრივ მიიღწევა შემთხვევითი მასკირების $x_1, x_2, \dots, x_\omega$ გადანაწილებით ω წილებზე და საბოლოო ნაწილი ანგარიშდება შემდეგნაირად: $x - (x_1 + x_2 + \cdots + x_\omega)$ არითმეტიკული ნიღბისთვის ან თუკი ლოგიკურ მასკირებასთან გვაქვს საქმე ამ წესით $x \oplus x_1 \oplus x_2 \oplus \dots \oplus x_\omega$. [42].

5. კიბერის უახლესი იმპლემენტაცია

კიბერის პოსტ-კვანტური კრიპტოგრაფიის ალგორითმმა, რომელიც რეკომენდირებულია NIST-ის მიერ, მნიშვნელოვანი პროგრესი განიცადა დანერგვის პროცესში. უახლესი კვლევები მიზნად ისახავს კიბერის მუშაობისა და ეფექტურობის გაუმჯობესებას ინოვაციური აპარატიული (hardware) დიზაინის გამოყენებით.

კვლევებმა შემოიტანა სპეციალური მოწყობილობები, აპარატურის ამაჩქარებლები და FPGA დანერგვები [43] პოლინომიური ოპერაციებისა და მოდულარული არითმეტიკის დასაჩქარებლად. ისინი გადამწყვეტია კიბერის დაშიფვრისა და გაშიფვრისთვის. ერთ–ერთი მაგალითია CRYPHTOR არქიტექტურა, რომელიც მოიცავს სპეციფიკურ ALU-ებს და მეხსიერების კონფიგურაციებს კიბერისა და Dilithium ალგორითმებისთვის [44]. CRYPHTOR ინტეგრირებულია 64-ბიტიან და 32-ბიტიან RISC-V-ზე დაფუძნებულ სისტემებში ჩიპზე (SoCs), რაც ძალიან დიდ სისწრაფეს აღწევს: 26-მდე რიცხვის თეორიული ტრანსფორმაციის (NTT) ოპერაციებისთვის და 140-მდე მატრიცა-ვექტორის ნამრავლისას.

FPGA-ის იმპლემენტაციებმა ასევე აჩვენეს წარმადობის მნიშვნელოვანი გაუმჯობესება მათი პარალელურობისა და ხელახალი კონფიგურაციის გამოყენებით, რაც აჩქარებს პოლინომიურ გამრავლებას, მოდულურ არითმეტიკას და კიბერისთვის სხვა არსებით ოპერაციებს. მკვლევარებმა შეიმუშავეს ახალი აპარატურის დიზაინი და ტექნიკა ამ ოპერაციების დასაჩქარებლად [45].

შესამჩნევი მიღწევაა სწრაფი აპარატურის დიზაინის შემუშავება პოლინომიური გამრავლებისთვის NTT-ის გამოყენებით CRYSTAL-Kyber და CRYSTAL-Dilithium-ში. ამ შემთხვევებში ვიყენებთ ციფრული სიგნალის დამუშავების (DSP) მიდგომებს [46]. ეს დიზაინები ამცირებს კრიტიკული გზის შეფერხებებს და აუმჯობესებს გარემოს და შესრულებას გამოყოფილი DSP ერთეულებით.

ასევე, მეცნიერები მუშაობენ კიბერის ეფექტურობის გასაუმჯობესებლად კომპაქტური ინსტრუქციების ნაკრების გაფართოებით და გაუმჯობესებული მოდულური გამრავლების მეთოდებით [47], რაც საშუალებას მისცემს კიბერს ეფექტურად შეძლოს მუშაობა რესურსებით შეზღუდულ მოწყობილობებზე.

მიუხედავად იმისა, რომ აპარატურების ამ მიღწევებმა გაზარდა გამოყენებადობა, უსაფრთხოება რჩება მთავარ პრიორიტეტად. უახლესმა კვლევებმა გვიჩვენა დაუცველობა გვერდითი არხის თავდასხმების მიმართ, სადაც თავდამსხმელები იყენებენ გვერდითი არხის ინფორმაციას, დაშიფვრის გასაღებების ამოსაღებად. ამ საფრთხეების დასაძლევად მკვლევარებმა შემოგვთავაზეს მიდგომები, როგორიცაა რეკურსიული სწავლება და მასკირების გამოყენება უსაფრთხოების გასაძლიერებლად [48]. გარდა ამისა, ახალი კრიპტოგრაფიული შედეგები, როგორიცაა მასკირებული პოლინომიური ოპერაციები და გასაღების დერივაციის გაუმჯობესებული პროცედურები [49], შესწავლილია კიბერის უსაფრთხოების გასაძლიერებლად, რომელიც დაგვიცავს პოტენციური თავდასხმებისგან.

6. შეტევები CRYSTALS–კიბერზე

NIST-მა რეკომენდაცია გაუწია CRYSTALS-კიბერს პოსტ–კვანტური დაშიფვრისთვის. მკვლევარებმა წარმატებით გამოიყენეს გვერდითი არხის თავდასხმები, ისარგებლეს ენერგიის მოხმარების მონაცემებით და ეს გამოადგად ალგორითმის მუშაობის პროცესის გასარღვევად, დაშიფვრის გასაღების გამოსავლენად. კონკრეტულად ამ შეტევაში, CRYSTALS-კიბერის შემთხვევაში გამოიყენეს მანქანური სწავლება ენერგიის რყევების გასაანალიზებლად, რაც ახლაც მზარდი უსაფრთხოების პრობლემაა.

მიუხედავად ამისა, CRYSTALS-Kyber არ ითვლება რომ არის "გატეხილი" ან "დანგრეული". ასეთი თავდასხმების ალბათობა რეალურ სამყაროში დაბალია. თუმცა, ეს ინციდენტი ხაზს უსვამს უსაფრთხოების ისეთი პოტენციური საფრთხეების ინფორმირებულობის აუცილებლობას. უახლესი შეტევები განვითარდა და გამოწვეულია მანქანური სწავლებით. ალგორითმი დაცულია და არ არის საჭირო ზედმეტად ღელვა მის უსაფრთხოებაზე.

წინა კვლევები იყენებდა AI-ს პირველი, მეორე და მესამე რიგის მასკირებული კიბერის იმპლემენტაციების დასარღვევად, მაგრამ უფრო მაღალი დონის მასკების გატეხვა ტრადიციული მეთოდებით გატეხვა რთულია, ასევე ტრადიციული AI მეთოდებითათ. Dubrova et al. დაძლიეს ეს პრობლემა ღრმა სწავლის ახალი ტექნიკისა და შეტყობინებების ბრუნვის გამოყენებით, ბიტის გაჟონვის გაზრდის მიზნით, რაც აძლიერებს შეტევების წარმატებას [50]. მათ მეთოდი აჩვენეს კიბერის პირველი რიგის მასკირების C ვერსიაზე, გააფართოვეს იგი უფრო მაღალი დონის მასკირების შემთხვევებისთვის და გააანალიზეს ენერგიის მოხმარება კიბერის ხელახალი დაშიფვრის ფაზაში.

თავდამსხმელის შეტევა ხდება დეკაფსულაციის სტადიის შემდეგ. საზიარო გასაღების ამოღების შემდეგ, ის ხელახლა იქმნება დეკაფსულაციის პროცესში და მოწმდება ორიგინალური დაშიფრული ტექსტის არის თუ არა შეცვლილი. საიდუმლო, ან საერთო გასაღების წინამორბედი, ბიტ–ბიტებით ინახება პოლინომში ხელახალი დაშიფვრის პროცესისთვის. უფრო კონკრეტულად, 256-ბიტიანი საიდუმლო უნდა გარდაიქმნას მრავალწევრიან მოდულად $q = 3329$, რომელიც არის 256 კოეფიციენტით, სადაც i-ური კოეფიციენტი უდრის $(q-1)/2$ იმ შემთხვევაში, როდესაც i-ური ბიტი არის 1, ხოლო 0 სხვა შემთხვევაში. მიუხედავად იმისა, რომ ფუნქცია მარტივი ჩანს, შესაძლოა რთული იყოს მასკირებული ვერსიის შექმნა. პრობლემა არის ის, რომ ნაწილები, რომლებიც ერთად ქმნიან საიდუმლოს, არის ბუნებრივი მეთოდი საიდუმლოების ნაწილების წარმოებისთვის, ისევე როგორც ნაწილები, რომლებიც ერთად ემატება მრავალწევრს, არის პოლინომიალის გაზიარების ბუნებრივი გზა.

სხვა კვლევებისგან განსხვავებით, ამ შემთხვევაში AI იყენებს რეკურსიულ სწავლებას პროფილირების ფაზის დროს, არსებითად, w - რიგის მასკირებული იმპლემენტაციის სწავლება გულისხმობს M^{w-1} მოდელის Batch ნორმალიზების ფენის წონების დუბლირებას, რომელიც მომზადებულია $(w-1)$ რიგის მასკირებულ იმპლემენტაციაზე. ამის შემდეგ შრე ფართოვდება, რომ მივითოთ საწყისი ქსელის M^w. რეკურსიული სწავლება გამოიყენება იმ შემთხვევაში, როდესაც მასკირებით შრეების რაოდენობა სამზე მეტია ანუ $w > 3$. უფრო

მცირე მასკირების რიგის შემთხვევაში შესაძლებელია გამოვიყენოთ ჩვეულებრივი მანქანური სწავლება და არ მოითხოვს ახალი რეკურსიული მიდგომის გამოყენებას. ამ მეთოდში AI–ის სწავლება ხდება ქსელის გამოყენებით ჩვეულებრივი შემთხვევითი წონის განაწილებით, როდესაც $w \leq 3$.

ორი უნივერსალური მოდელი, M_0^w და M_1^w მიიღება ბაიტის მიხედვით დაჭრის და შეერთების სასწავლო კვალის გამოყენებით. ეს პროცესი აღადგენს ყველაზე ძლიერი გაჟონვის ადგილს, რომელიც არის თითოეული შეტყობინების ბაიტის პირველი და მეორე ბიტი. ესე იგი, შეტყობინების პირველ ნაწილში უფრო მეტი ინფორმაცია გაიჟონება ვიდრე ბოლო ნაწილში. გარდა ამისა, შეტყობინებების ბიტები "0" და "1" გამოიყენება როგორც ეტიკეტები და AI-ებს ასწავლიან შეტყობინების მიღებას პირდაპირ, ყოველი გამეორების დროს შემთხვევითი მასკირებების მოხსნის გარეშე.

თითოეული ბაიტის ბოლო ექვსი ბიტი გადაინაცვლებს პირველი ორი ბიტის პოზიციებზე მას შემდეგ, რაც შეტყობინება სამჯერ შემობრუნდება. ეს მეთოდი ეხმარება ბიტის მნიშვნელობების უფრო საიმედოდ ამოღებას „უფრო გაჟონვის“ ბიტების მდებარეობების გამოყენებით, რაც ზრდის შეტევის წარმატების კოეფიციენტს.

თავდასხმის ეტაპი იყენებს ციკლური როტაციის მიდგომას. ეს გამოიყენება masked_poly_frommsg()–დან გაჟონვის არაერთგვაროვანი განაწილების გამო, რაც გამოიხატება 0-დან 7-მდე ბიტებს შორის წარმატებული აღდგენის ალბათობის 9%-იანი შეუსაბამობით. მოცემული module-LWEs არის ring-LWE-ების გაფართოებები, რომელთა დაშიფრული ტექსტები შეიძლება შეიცვალოს მათი შეტყობინებების ციკლურად როტაციისთვის. თითოეული ბაიტის ბოლო 6 ბიტი საწყის 2 ბიტზე გადაბრუნებით, შეტევა აბრუნებს შეტყობინებას ნეგაციკლურად სამჯერ, 2 ბიტით. ეს საშუალებას აძლევს ბიტებს გაჟონოს მეტი ინფორმაცია ზედმეტი დროის გამოყენების გარეშე, სხვა ციკლური მიდგომებისგან განსხვავებით.

შესატყვისი დაშიფრული ტექსტის მანიპულირება საშუალებას აძლევს ადამიანს შეცვალოს შეტყობინება. პოლინომები რგოლში $\mathbb{Z}_q[X]/(X^{256}+1)$ ქმნის დაშიფრულ ტექსტს $c = (u, v)$ CRYSTALS-Kyber-ში. შეტყობინების ნეგაციკლური როტაცია შეიძლება მივიღოთ u-ს და v-ის გამრავლებით განუსაზღვრელ X-ზე, იმ პირობით, რომ c სწორად არის შექმნილი. Decode (-y) და decode (y) შეიძლება შევაფასოთ სხვადასხვა მნიშვნელობებით, ამის გამო ამ მიდგომამ შეიძლება გამოიწვიოს შეცდომები საიდუმლო გასაღების აღდგენის მცდელობებში, როდესაც გამოვიყენებთ კონკრეტული დაშიფრული ტექსტებისთვის [51-52].

გაყოფილი ორი ნაწილი შემოიფარგლება კოდით. ის ქმნის მასკას ყოველი ბიტისთვის, რომელიც არის 0xffff, თუ ბიტი იყო 1, ხოლო 0 სხვა შემთხვევაში. საჭიროების შემთხვევაში, ეს ნიღაბი გამოიყენება მრავალწევრის, პოლინომიალის წილის გასაზრდელად $(q+1)/2$-ით. 1-ის დასამუშავებლად მას ცოტა მეტი ელექტროენერგია დასჭირდება. AI არ არის საჭირო იმის დასადგენად, რომ ეს ფუნქცია გაჟონავს. ეს სიტუაცია აღინიშნა 2016 წელს, რომ ეს პატერნი ცუდი იყო. 2020 წელს კი გამოჩნდა, რომ შესაძლოა არსებობდეს ფარული კიბერის

რისკი. როგორც შესაბამისი საპასუხო ღონისძიება, მრავალი ბიტის ერთდროულად დამუშავება არის ერთ-ერთი ტექნიკა ამის შესამცირებლად.

ავტორები, Dubrova და სხვები არ ამტკიცებენ, რომ ეს არის რადიკალურად ახალი თავდასხმა. პირიქით, ისინი აძლიერებენ თავდასხმის ეფექტურობას ორი გზით: ნერვული ქსელის სწავლებით და იმის გარკვევით, თუ როგორ შეიძლება უკეთესად გამოვიყენოთ მრავალი გზა/ბილიკი გაგზავნილი დაშიფრული ტექსტის შეცვლით. ავტორებმა გამოსცადეს შემოთავაზებული შეტევა შემდეგ მოწყობილობაზე: გამოიყენეს ARM Cortex-M4 CPU, რომელსაც გააჩნია STM32F415-RGT6 მოწყობილობა, CW308 UFO დაფა და CW308T-STM32F4 სამიზნე დაფა, რომელიც მუშაობს 24 MHz-ზე, ენერგიის მოხმარება იზომება მაღალი 10-ბიტიანი სიზუსტით 24 MHz.

ნერვული ქსელების მომზადების მიზნით, გროვდება 150,000 დენის კვალი სხვადასხვა დაშიფრული ტექსტების გაშიფვრისთვის ერთი და იგივე KEM გასაღების წყვილისთვის (ცნობილი საერთო გასაღებით). რეალურ სამყაროში თუ გვინდა მსგავსი თავდასხმა, ეს უკვე უჩვეულოა, რადგან საკვანძო შეთანხმებებისთვის KEM გასაღების წყვილები დროებითია, რაც ნიშნავს, რომ ისინი იქმნება და გამოიყენება მხოლოდ ერთხელ. თუმცა, გრძელვადიანი KEM გასაღების წყვილებს აქვთ რამდენიმე მოქმედი აპლიკაცია, მათ შორის ECH, HPKE და ავტორიზაცია.

გაწვრთნა გადამწყვეტია, რადგან ერთი და იგივე ბრენდისა და მოდელის მოწყობილობებსაც კი შეუძლიათ აჩვენონ სხვადასხვა სიმძლავრის კვალი ერთი და იგივე კოდის გაშვებისას. ნერვული ქსელების ვარჯიში, სწავლება აუცილებელია. ვწრთვნით შეტევაზე „ნაწილების“ ან იმპლემენტაციების უსაფრთხოების სხვადასხვა დონეზე. ექვს ნაწილად გაყოფილი (ანუ მასკირების მეხუთე დონე) იმპლემენტაციის შეტევისთვის, ძალაუფლების კვალის მეხუთედი მოდის ექვსწილიანი განხორციელებიდან, მეხუთედი ხუთ წილიდან და ა.შ. ნაკლებად სავარაუდოა, რომ ვინმემ გამოიყენოს მოწყობილობა, რომელიც საშუალებას აძლევს შეცვალოს გაზიარებული რიცხვები.

როგორც ავტორებმა აღნიშნეს, ფაქტობრივი შეტევა იწყება იმით, რომ იდეალურ პირობებში მათ შეეძლოთ საერთო გასაღების ამოღება ორი ნაწილიანი დეკაფსულაციის ერთი სიმძლავრის კვალიდან. გასაღების ამოღების შანსი არის 0,127%. ისინი არ გვაძლევენ რიცხვით ინფორმაციას ორზე მეტ აქციაზე ერთი კვალის ნაშალიდან (shares).

გვერდითი არხის თავდასხმები უფრო წარმატებულია ერთი და იგივე დეკაფსულაციის მრავალი კვალით. ერთი და იმავე შეტყობინების კვალის დატოვების ნაცვლად, ავტორები ატრიალებენ დაშიფრულ ტექსტს. ეს ზრდის წარმატების კოეფიციენტს 78%-მდე ოთხი კვალის, ორი წილის იმპლემენტაციისთვის. ექვსი ნაწილი გაყოფის შემთხვევაში იმპლემენტაცია კვლავ ძლიერია, 0.5%. როდესაც დაშვებულია 20 კვალის, გზის ექვსწილიანი იმპლემენტაციიდან, საზიარო გასაღების 87% შეიძლება აღვადგინოთ.

2.5 K შეტყობინებები არჩეულია შემთხვევით ყოველი w-რიგის ნიღბიანი, მასკირებული განხორციელებისთვის. ვინაიდან თითოეული კვალი შეიცავს სამი 2-ბიტიანი ციკლური შეტყობინების ბრუნვას, სულ არის 10 K კვალი თითოეული შეტყობინებისთვის., თუკი არ

გამოვიყენებთ ციკლურ ბრუნვას/როტაციას. შეტყობინების აღდგენის საშუალო ალბათობა პირველი რიგის მასკირებული განხორციელებისთვის ერთი კვალით არის 0,127%. ციკლური ბრუნვები ზრდის ამ შანსს 78,866%-მდე. ალბათობა არის 0.56% მეხუთე რიგის მასკირებულ განხორციელებაზე ციკლური ბრუნვის გამოყენებით ერთი კვალის შემთხვევაში, 54.53% სამი კვალის და 87.085% ხუთი კვალის შემთხვევაში.

ტექნიკის თვალსაზრისით, ის შეიძლება გარკვეულწილად წააგავდეს სმარტ ბარათს, მაგრამ მნიშვნელოვნად განსხვავდება მაღალი დონის გაჯეტებისგან, როგორიცაა დესკტოპის კომპიუტერები, სერვერები და მობილური ტელეფონები. უბრალოდ ინტეგრირებული 1 გიგაჰერციანი პროცესორების პირობებშიც კი, გვერდითი არხის მარტივი ანალიზის თავდასხმები გაცილებით რთულია, მათ სჭირდებათ ათიათასობით კვალი პროცესორთან ახლოს განთავსებული მაღალი დონის ოსცილოსკოპით. სერვერზე ამ ტიპის ფიზიკური წვდომა გვთავაზობს ბევრად უკეთეს შეტევის ვექტორებს; ამისთვის მხოლოდ საჭიროა დავაკავშიროთ ოსცილოსკოპი მეხსიერებას (memory bus).

ელექტროენერგიის არხზე თავდასხმები ზოგადად განიხილება, როგორც არარიალიზებადი, გარდა უკიდურესად მგრძნობიარე აპლიკაციებისა. თუმცა, დახშობამ შეიძლება ზოგჯერ გამოიწვიოს ძალზე ძლიერი გვერდითი არხის თავდასხმა, რომელიც გადაიქცევა დისტანციური დროის შეტევად (distant timing attack). მტკიცედ რომ ვთქვათ, ეს შეტევა ახლოსაც არ არის იმასთან, რაც ხდება.

გარდა ამისა, ეს შეტევა არ არის ძალიან ძლიერი ან მოულოდნელი, თუნდაც გარკვეული მგრძნობიარე აპლიკაციებისთვის, როგორიცაა ჭკვიანი ბარათები. პრაქტიკაში, არ აქვს მნიშვნელობა, შენიღბული იმპლემენტაცია გაამჟღავნებს თუ არა თავის საიდუმლოებას - ის ყოველთვის აკეთებს. საკითხავია, რამდენად რთულია რეალურ ცხოვრებაში ამ შეტევის შესრულება და უღირს თუ არა თავდამსხმელს მასზე დროის დაკარგვა. მსგავსი სტატიები ეხმარება მწარმოებლებს განსაზღვრონ რამდენი საპასუხო ღონისძიება გამოიყენონ, რათა მსგავსი სტილის თავდასხმების რეალურ გარემოში შესრულება რთული და უზომოდ ძვირი იყოს.

7. საწინააღმდეგო ზომები

არსებული თავდასხმების უმრავლესობისგან საუკეთესო დაცვა არის აპლიკაციის საიდუმლო გასაღების ხანგრძლივობის შემცირება. თავდასხმა უფრო რთული იქნება, რაც უფრო ნაკლები იქნება საიდუმლო გასაღები საჯარო. თავდამსხმელს შეუძლია გამოიყენოს შეტყობინების აღდგენის შეტევა მხოლოდ იმ შემთხვევაში, თუ საიდუმლო გასაღები გამოიყენება მხოლოდ ერთხელ. თუმცა, ამან შეიძლება გამოიწვიოს სხვა პრობლემებიც. მაგალითად, შეიძლება საჭირო გახდეს საიდუმლო გასაღებების დიდი რაოდენობის შექმნა, თუ არა საიდუმლო გასაღებების გამოყენება აღმოიფხვრება.

თუკი შეუძლებელია დეკაფსულაციის პროცედურის განმეორებით ჩატარება, მოცემული შეტევა წარმატებით ვერ შესრულდება. შეზღუდვა, რამდენჯერ შეიძლება მოხდეს ერთი და იგივე შიფრული ტექსტის დეკაფსულაცია იმავე საიდუმლო გასაღებით, დაგვეხმარება ამის

მიღწევაში. შეიძლება დაგჭირდეს რამდენიმე გამეორების დაშვება, რათა მიიღოთ შემთხვევითი კომუნიკაციის შეცდომები (andom communication errors).

ალტერნატივად შეიძლება გამოვიყენოთ უფრო ძლიერი დაცვის სისტემები სიმძლავრის ანალიზის თავდასხმებისგან, როგორიცაა: დუბლირება საათის რანდომიზაციის მიდგომა (duplication with clock randomization approach) [53]. მთავარი და მოჩვენებითი კრიპტოგრაფიული ბირთვი არის ორი იდენტური ბირთვი, რომლებიც ქმნის დაცულ იმპლემენტაციას. მიუხედავად იმისა, რომ ორი ბირთვი იყენებს ორ განსხვავებულ საიდუმლო და საჯარო გასაღების წყვილს მათი შესაბამისი ამოცანებისთვის, მათ აკონტროლებს ორი განსხვავებული რანდომიზირებული საათი და იღებენ იდენტურ შეყვანის მონაცემებს. ასეთ ტექნიკას აქვს შემდეგი უპირატესობები თუკი მასკირებას შევადარებთ: ნულოვანი საათის ციკლის ზედმეტად, იმუნიტეტი ხარვეზების მიმართ, უნივერსალური დაფარვა და უფრო მაღალი გამძლეობა განმეორებითი თავდასხმების მიმართ.

8. დასკვნა

შემოთავაზებული გასაღების ინკაფსულაციის სისტემა, CRYSTALS-Kyber, მზარდი სირთულეების წინაშე დგას სხვადასხვა გვერდითი არხის თავდასხმების გამო. მიმდინარე კვლევები ავლენს სისუსტეებს ძლიერი უსაფრთხოების შემთხვევაშიც კი, რაც მოითხოვს მუდმივად დაცვის სისტემების გაუმჯობესებას. მასკირება და არევა (shuffling) არის ორი საწინააღმდეგო ღონისძიება, რომლებიც აუცილებელია კრიპტოგრაფიული სისტემების გასაძლიერებლად. როდესაც ჩვენ ვუახლოვდებით პოსტ–კვანტურ ეპოქას, აუცილებელია შევაფასოთ ალფორითმები, როგორც მათემატიკური სიძლიერისთვის, ასევე გვერდითი არხის თავდასხმებისადმი მდგრადობისთვის.

დაშიფვრის ახალი მეთოდების სრულად გარღვევის ნაცვლად, AI-ს შეუძლია დაეხმაროს ხმაურიანი მონაცემების მართვაში და ელექტროენერგიის გვერდითი არხის თავდასხმა და პირდაპირი კრიპტოგრაფიის დარღვევა ძალიან განსხვავდება ერთმანეთისგან. მიუხედავად იმისა, რომ ფაქტობრივი შეტევები იყენებს რამდენიმე კვალს, ღრმა სწავლას შეუძლია ივარჯიშოს ძალიან ხმაურიან კვალზე. ამ დისკუსიის საინტერესო ნაწილი ის არის, რომ პირდაპირი, ხელმისაწვდომი და ეფექტური თავდაცვითი საშუალებების ნაკლებობა გვაქვს ძლიერი, გვერდითი არხის თავდასხმების შესაჩერებლად.

9. დადასტურება/აღიარება

კვლევა [NFR-22-14060] განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით.

ბიბლიოგრაფია

1. Buchmann, J., Dahmen, E., Szydlo, M. (2009). Hash-based Digital Signature Schemes. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_3
2. Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
3. Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41, no. 2 (1999): 303-332.
4. Iavich, Maksim, et al. "ADVANTAGES AND CHALLENGES OF QRNG INTEGRATION INTO MERKLE." Scientific and practical cyber security journal (2020).
5. Gagnidze, Avtandil, Maksim Iavich, and Giorgi Iashvili. "Novel version of merkle cryptosystem." Bulletin of the Georgian National Academy of Sciences (2017).
6. Iavich, M., Kuchukhidze, T., & Bocu, R. (2023). A Post-Quantum Digital Signature Using Verkle Trees and Lattices. Symmetry, 15(12), 2165.
7. Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST (2022).
8. Announcing the commercial national security algorithm suite 2.0. National Security Agency, U.S Department of Defense https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
9. Avanzi, Roberto, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Kyber algorithm specifications and supporting documentation." NIST PQC Round 2, no. 4 (2019): 1-43.
10. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Annual international cryptology conference. pp. 388–397. Springer (1999)
11. Wu, L., Perin, G., Picek, S. (2022). On the Evaluation of Deep Learning-Based Side-Channel Analysis. In: Balasch, J., O'Flynn, C. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2022. Lecture Notes in Computer Science, vol 13211. Springer, Cham. https://doi.org/10.1007/978-3-030-99766-3_3
12. Wang, R., Ngo, K., Dubrova, E.: A message recovery attack on LWE/LWR-based PKE/KEMs using amplitude-modulated EM emanations. In: Proc. of 25th Annual Int. Conf. on Information Security and Cryptology (2022), https://eprint.iacr. org/2022/852
13. Fritzmann, T., Van Beirendonck, M., Basu Roy, D., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2021). Masked accelerators and instruction set extensions for post-quantum cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(1), 414-460.
14. Gigerl, B., Primas, R., & Mangard, S. (2023, May). Formal verification of arithmetic masking in hardware and software. In International Conference on Applied Cryptography and Network Security (pp. 3-32). Cham: Springer Nature Switzerland.
15. Coron, J. S., Gérard, F., Montoya, S., & Zeitoun, R. (2021). High-order polynomial comparison and masking lattice-based encryption. Cryptology ePrint Archive.
16. Ngo, K., Dubrova, E., Johansson, T.: Breaking masked and shuffled CCA secure Saber KEM by power analysis. In: Proc. of the 5th Workshop on Attacks and Solutions in Hardware Security. pp. 51–61 (2021)
17. Kairouz, P., McMahan, B., Song, S., Thakkar, O., Thakurta, A., & Xu, Z. (2021, July). Practical and private (deep) learning without sampling or shuffling. In International Conference on Machine Learning (pp. 5213-5225). PMLR.

18. Nguyen, T. T., Trahay, F., Domke, J., Drozd, A., Vatai, E., Liao, J., ... & Gerofi, B. (2022, May). Why globally re-shuffle? Revisiting data shuffling in large scale deep learning. In 2022 IEEE International Parallel and Distributed Processing Symposium (IPDPS) (pp. 1085-1096). IEEE.
19. Brisfors, M., Moraitis, M., & Dubrova, E. (2022). Side-channel attack countermeasures based on clock randomization have a fundamental flaw. Cryptology ePrint Archive.
20. Jayasinghe, D., Udugama, B., & Parameswaran, S. (2023, January). FPGA Based Countermeasures Against Side channel Attacks on Block Ciphers. In Proceedings of the 28th Asia and South Pacific Design Automation Conference (pp. 365-371).
21. Coron, Jean-Sébastien, and Ilya Kizhvatov. "An efficient method for random delay generation in embedded software." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 156-170. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.
22. Leplus, G., Savry, O., & Bossuet, L. (2022, June). Insertion of random delay with context-aware dummy instructions generator in a RISC-V processor. In 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 81-84). IEEE.
23. Xagawa, K., Ito, A., Ueno, R., Takahashi, J., & Homma, N. (2021). Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates. In Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27 (pp. 33-61). Springer International Publishing.
24. Maghrebi, H., Servant, V., & Bringer, J. (2016). There is wisdom in harnessing the strengths of your enemy: Customized encoding to thwart side-channel attacks. In Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers 23 (pp. 223-243). Springer Berlin Heidelberg.
25. Belleville, N., Couroussé, D., Heydemann, K., & Charles, H. P. (2018). Automated software protection for the masses against side-channel attacks. ACM Transactions on Architecture and Code Optimization (TACO), 15(4), 1-27.
26. Kreuzer, K. (2023). Verification of Correctness and Security Properties for CRYSTALS-KYBER. Cryptology ePrint Archive.
27. Wang, Z., Meng, F. H., Park, Y., Eshraghian, J. K., & Lu, W. D. (2023). Side-channel attack analysis on in-memory computing architectures. IEEE Transactions on Emerging Topics in Computing.
28. Moraitis, M., Ji, Y., Brisfors, M., Dubrova, E., & Lindskog, N. (2023). Securing CRYSTALS-Kyber in FPGA Using Duplication and Clock Randomization. IEEE Design & Test.
29. Jeon, H., Xie, J., Jeon, Y., Jung, K. J., Gupta, A., Chang, W., & Chung, D. (2023). Statistical power analysis for designing bulk, single-cell, and spatial transcriptomics experiments: review, tutorial, and perspectives. Biomolecules, 13(2), 221.
30. Zulberti, L., Di Matteo, S., Nannipieri, P., Saponara, S., & Fanucci, L. (2022). A script-based cycle-true verification framework to speed-up hardware and software co-design: Performance evaluation on ecc accelerator use-case. Electronics, 11(22), 3704.
31. Köpf, B., & Dürmuth, M. (2009, July). A provably secure and efficient countermeasure against timing attacks. In 2009 22nd IEEE Computer Security Foundations Symposium (pp. 324-335). IEEE.
32. He, J., Guo, X., Tehranipoor, M. M., Vassilev, A., & Jin, Y. (2022). EM Side Channels in Hardware Security: Attacks and Defenses. IEEE Des. Test, 39(2), 100-111.
33. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. IEEE Access.
34. Hofheinz, Dennis, Kathrin Hövelmanns, and Eike Kiltz. "A modular analysis of the Fujisaki-Okamoto transformation." In Theory of Cryptography Conference, pp. 341-371. Cham: Springer International Publishing, 2017.

35. Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." In Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16, pp. 104-113. Springer Berlin Heidelberg, 1996.
36. Ngo, Kalle, Elena Dubrova, Qian Guo, and Thomas Johansson. "A side-channel attack on a masked IND-CCA secure saber KEM implementation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 676-707.
37. Bhasin, Shivam, Jan-Pieter D'Anvers, Daniel Heinz, Thomas Pöppelmann, and Michiel Van Beirendonck. "Attacking and defending masked polynomial comparison for lattice-based cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 334-359.
38. Guo, Q., Nabokov, D., Nilsson, A., & Johansson, T. (2023, December). Sca-ldpc: A code-based framework for key-recovery side-channel attacks on post-quantum encryption schemes. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 203-236). Singapore: Springer Nature Singapore.
39. Xu, Zhuang, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers 71, no. 9 (2021): 2163-2176.
40. Ravi, Prasanna, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "Drop by Drop you break the rock-Exploiting generic vulnerabilities in Lattice-based PKE/KEMs using EM-based Physical Attacks." IACR Cryptol. ePrint Arch. 2020 (2020): 549.
41. Beirendonck, Michiel Van, Jan-Pieter D'anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. "A side-channel-resistant implementation of SABER." ACM Journal on Emerging Technologies in Computing Systems (JETC) 17, no. 2 (2021): 1-26.
42. Ngo, Kalle, Elena Dubrova, Qian Guo, and Thomas Johansson. "A side-channel attack on a masked IND-CCA secure saber KEM implementation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 676-707.
43. Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021). Instruction-set accelerated implementation of CRYSTALS-Kyber. IEEE Transactions on Circuits and Systems I: Regular Papers, 68(11), 4648-4659.
44. Di Matteo, S., Sarno, I., & Saponara, S. (2024). CRYPHTOR: A Memory-Unified NTT-Based Hardware Accelerator for Post-Quantum CRYSTALS Algorithms. IEEE Access, 12, 25501-25511.
45. Nguyen, T. H., Kieu-Do-Nguyen, B., Pham, C. K., & Hoang, T. T. (2024). High-speed NTT Accelerator for CRYSTAL-Kyber and CRYSTAL-Dilithium. IEEE Access.
46. Wang, H., Zhou, J., Xing, Z., Feng, Q., Zhang, K., Zheng, K., ... & Li, Z. (2023). Fast-convergence digital signal processing for coherent PON using digital SCM. Journal of Lightwave Technology, 41(14), 4635-4643.
47. Li, L., Qin, G., Yu, Y., & Wang, W. (2023). Compact Instruction Set Extensions for Kyber. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
48. Zhao, Y., Pan, S., Ma, H., Gao, Y., Song, X., He, J., & Jin, Y. (2023). Side channel security oriented evaluation and protection on hardware implementations of kyber. IEEE Transactions on Circuits and Systems I: Regular Papers.
49. Kundu, S., Karmakar, A., & Verbauwhede, I. (2023, December). On the Masking-Friendly Designs for Post-quantum Cryptography. In International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 162-184). Cham: Springer Nature Switzerland.
50. Dubrova, Elena, Kalle Ngo, Joel Gärtner, and Ruize Wang. "Breaking a fifth-order masked implementation of crystals-kyber by copy-paste." In Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop, pp. 10-20. 2023.

51. Azouaoui, Melissa, Yulia Kuzovkova, Tobias Schneider, and Christine van Vredendaal. "Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks." Cryptology ePrint Archive (2022).
52. Backlund, Linus, Kalle Ngo, Joel Gärtner, and Elena Dubrova. "Secret Key Recovery Attack on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber." In International Conference on Applied Cryptography and Network Security, pp. 159-177. Cham: Springer Nature Switzerland, 2023.
53. Nikova, Svetla, Christian Rechberger, and Vincent Rijmen. "Threshold implementations against side-channel attacks and glitches." In International conference on information and communications security, pp. 529-545. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 53 – 64 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MODERN NETWORK WARS

Volodymyr Khoroshko[1], Volodymyr Artemov[2], Mykolay Brailovskyi[3], Valeri Kozura[2]

[1]National Aviation University, Kyiv, Ukraine
[2]National Security Academy, Kyiv, Ukraine
[3]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT: The article examines the theory of network-centric warfare and its impact on the present. It was developed in the second half of the twentieth century and is widely used in the wars of the twenty-first century. The essence of the concept of network-centric warfare can be redefined as follows: it is a war of the "blind" against the "sighted". The physical strength of the "blind man" is the combat strength of classical armed forces that do not take advantage of network-centric approaches, which does not guarantee an advantage in modern combat. This is a losing situation. Network-centric warfare consists of 3 lattice subsystems: information, sensor (i.e., intelligence) and combat. But its basis is the information subsystem, the goals of which, according to the concept, are the so-called Warden rings. Using the theory of network-centric warfare and hybrid warfare tactics, Russia seized Crimea and occupied Donbas. And on 24 February 2024, Russia launched a war against Ukraine, repeating its actions during the aggression against Georgia in 2008. That is, it started with cyberattacks on government agencies and government control centres. But the Russian Federation, using elements of network-centric warfare, is fighting as it did in World War II. Ukraine is making a transition from managing troops and weapons to managing armed struggle. Russia's war against Ukraine shows that in modern warfare, the winner is the one who is quicker to perceive new technologies and implement them, adopts and implements new military doctrines and concepts that are in line with the spirit of the times and enable not only the use of new technologies and ideas, but also knows well which ones to use and when. High technologies are now turning into a systemic factor in modern armed struggle. They make it possible to reach that new stage in the development of military art - the transition from command and control of troops in the course of armed struggle to conflict management in general.

KEYWORDS: network-centric warfare, hybrid warfare, Warden rings, Boyd's theory.

1. INTRODUCTION

The existence and development of modern resources is closely linked to geopolitical and geostrategic conditions and largely depends on international relations. At the same time, increasing importance is being attached to ensuring national security - the state of protection of vital interests of an individual, society and the state from internal and external threats.

Among the many factors that influence the formation of foreign and domestic policy of states, national interests play a decisive role. National interests are understood at all levels of public life as the needs of the people of the country to preserve and increase national values and national wealth, economic prosperity and political stability of the society, and are reflected in the formation and achievement of national goals. Thus, national interests and actions to achieve them are linked. In interstate relations, not only such actions, but even their implementation are subject to increased attention, careful study and comprehensive assessment. This is especially true in Europe, where the intertwining of the interests of states in an overpopulated and technologically saturated territory is observed to the highest degree.

In addition, substantiating the national military security strategy is an important and responsible task. Strategic thinking is an integral factor of effective policy. As the famous military science theorist O. Svechin noted back in 1927: "Strategy is one of the most important tools of politics, and even in peacetime, politics

must largely base its calculations on the military capabilities of friendly and hostile states. The strategy should look into the future and take it into account in a very broad perspective."

The analysis of modern military conflicts provides a key to understanding the logic of the actions of participants in armed struggle anywhere in the world. However, this arsenal involves not only significant material costs, but also the political weight of the state that decided to use it. Current trends in the preparation and conduct of warfare today are as follows [1]:

- the expectation that the armed forces will be equipped with means of conducting non-contact warfare. Now there is no need to "go toe-to-toe" with a raised visor, as high-precision weapons, electronic intelligence and electronic warfare means are making their mark;
- Intensive build-up of rapid response forces, airborne troops and special forces. The readiness to win not through numerical superiority, but through skill and better equipment, in difficult conditions, surrounded by civilians, is becoming a necessity. Fighting not by numbers, but by skill, surrounded by civilians, is becoming a widely sought-after skill (but not for the Russian army);
- the desire to inflict defeat and demoralize the enemy in the rear with "little blood, one blow" using the factor of surprise;
- to transform the confrontation in the information sphere from an accompanying to a dominant sphere, moving from the desire to enter the territory of the country to the intention to purposefully influence and control the thoughts and emotions of its citizens;
- the spread of humanitarian interventions as the right of a more influential state in the world's pecking order to "take care" of the population of another country that has found itself in the sphere of the "patron's" interests.

The theory of network-centric warfare (NCW), which emerged at the turn of the second and third millennia, states that armed forces that implement network support (horizontal and single-ended) for all organizational forms and processes have an advantage over traditional forces. The general informatization and intellectualization of command-and-control systems will qualitatively change the essence of military operations, turning them into network-centered ones. It is not about the humanization of war; it is total and is conducted continuously and in all spheres of state functioning.

The NCW places its ultimate stake on information warfare. The term "information warfare" has evolved over time into the concept of "information warfare." Information warfare is a complex impact (through a set of information operations) on the system of state and military governance of the opposing party, its military and political leadership, which in peacetime can lead to decisions favorable to the party initiating the information influence, and in conflict completely paralyzes the functioning of the enemy's control infrastructure. Otherwise, the goal of war in the 21st century is not so much to destroy the enemy as to demoralize it and deprive it of the ability to resist.

Therefore, the world's leading powers ensure their defense capability, in accordance with existing and projected dangers and threats, mainly through the development and combination of modern high-tech means into a single integrated system and their implementation in the practice of using troops [2].

2. MAIN PART

Let us consider the history of the creation and development of the theory of network-centered warfare. For the first time, the conceptual issues and foundations of the theory of a network-centric system of control and organization of combat and cyber actions and, in fact, the consideration of military operations and their organization from the standpoint of military cybernetics were formulated by M. V. Ogarkov (1977-1984, Chief of the General Staff of the USSR Armed Forces) in the late 70s and early 80s of the twentieth century [3,4]. These provisions and conclusions of M. V. Ogarkov were implemented in the US military doctrines "JoinVision 2010" and "JoinVision 2020".

The main aspects of taking a state under external control to realize its interests by suppressing the will of the population and authorities of the victim country to resist through the use of a wide range of innovative technologies that are used in a comprehensive manner were described in 1989 in an article by William Lind.

The main thing in the wars of the fourth generation, according to W. Lind, is the war of cultures, initiation, support and feeding from the outside and organization of psychological and informational pressure on its people and leadership inside the country, taking them under external control and management, creating conditions for the emergence and promotion of socio-economic chaos in this country and self- depletion of military, financial and other resources. For this purpose, high-tech psychological actions, manipulation of the media, a wide range of information warfare actions, both inside the country and in the global media and Internet spaces, introduction of norms into national legislation that are harmful to national interests [5,6]. Targeted comprehensive aggressive attacks on traditional cultural, historical and other values of the population, on the reputation of the most effective key leaders of the state and state-military administration. Creating conditions for lowering the level of upbringing, culture, and education of citizens. Organizing campaigns of disobedience, implementing the tactics of "low-intensity conflicts" on the territory of the victim country with the participation of external, internal and terrorist forces.

A statement by the great Chinese commander Sun Tzu: "War loves victory and does not like duration. I have heard of the success of quick military campaigns and have not heard of the success of long ones. No state has ever benefited from a long war."

Based on this, American military experts have proposed a number of concepts of warfare. The most famous of them is Boyd's concept or theory. In his concept, Boyd divides war into three elements [7]:

- moral warfare: destroying the enemy's will to win by separating them from their allies (or potential allies) and dividing them internally, undermining their common faith and shared views;
- mental warfare: deformation and distortion of the enemy's perception of reality based on disinformation and creating a false picture of the situation;
- physical warfare: destruction of the enemy's physical resources (weapons, manpower, infrastructure).

According to the ideas of Boyd and his followers, any activity in the military sphere can be represented with a certain degree of approximation in the form of a cybernetic model of OODA (Observe, Orient, Decide, Act). This model assumes a repeated repetition of the action loop, consisting of four successive interacting processes: observation, orientation, decision, and action. In fact, the situation develops in a spiral, and at each stage of this spiral, interaction with the external environment is carried out and has an impact on the enemy. This model is classified as cybernetic, because it implements the principle of "feedback", according to which part of the output of the system is fed back to its input to clarify and, if necessary, adjust the development of the system in the following stages. In a number of official doctrinal documents of the US Department of Defense, the OODA loop is considered as the only typical model of the decision-making cycle for command-and-control systems (C2 systems), both for its own and enemy forces.

The distinctive feature of the OODA cycle from other cyclical models is that in any situation, it is always assumed that there is an enemy with whom an armed struggle is being waged. The enemy also acts and makes decisions within its own similar loop.

Based on the analysis of the works of Boyd and his followers, the following postulates of the OODA theory are highlighted:

1. The military activities of the opposing sides are carried out in the same cybernetic cycles of the OODA.
2. The content of the main elements of the OODA cycle is as follows:

- observation - collecting information from internal and external sources;
- orientation - the formation of a set of possible plans (options) and theevaluation of each of them according to a set of criteria;
- decision - choosing the best action plan for practical implementation;
- action - practical implementation of the selected action plan.

3. The OODA cycle is a model of military activities of individuals and organizations for war and conflicts of any level (tactical, operational and strategic).

4. Ways to achieve victory (gaining competitive advantages):
   - Reduction of the time for the OODA cycle;
   - improving the quality of decisions made in the cycle.
5. Increasing the speed of all the particles of the elements of the OODA cycle is the main way to achieve victory.

Out of the four stages of the OODA cycle, three are directly related to information processing and computer technology. The fourth stage (action) is generally of a "kinematic" nature and is associated with movement in space, defense and defeat of the enemy based on firepower.

In order to maintain the time frame of the OODA cycle of your forces' actions and ensure a higher tempo of combat than the enemy, it is necessary to accelerate all four stages of the cycle, which are implemented by troops. Throughout the twentieth century, all efforts of the military, scientists and engineers were aimed at improving weapons and technologies in the kinematic part of the OODA loop. These efforts resulted in increased mobility, accuracy and firepower of weapons. However, the technological limit of the kinematic part of the OODA loop has now been reached: more powerful weapons cause acceptable collateral damage, and faster and more protected weapon platforms and means of delivering the impactor to the target imply material costs that are prohibitive at the present stage. In this regard, there is a need to improve other stages of the OODA cycle.

Since the first three stages of the OODA cycle are directly related to the processes of collecting information, distributing it, comprehending, analyzing, and making decisions based on the information received, the faster the collection, distribution, analysis, and perception of information are carried out, the faster the decision is made. It is the speed and correctness of decision-making that are most important in today's real-world combat operations. This was the impetus for the development of the concept of network-centered military activities, or as it is also called network-centered warfare.

The issue of systemic disruption of the governance and functioning of the state at the pre-crisis level was proposed and implemented during the preparation of Operation Desert Storm in 1991 by John Warder. He developed a systematic cybernetic approach to modern warfare, calling it "effects-based operations" (EBO), which took into account Boyd's developments and became a further development of the cybernetic concept of network-centric organization of combat operations with elements of the theory of constraint. According to this concept, there are five main segments: armed forces, production, infrastructure and communications, population and government - vital for any state. Each state has its own unique points of vulnerability in them (called "centers of gravity", "critical points", etc.). Their correct detection and destructive impact on them lead to the effect of systemic "paralysis" of the state in certain areas or in general. This technology was used by Russia in 2014 during the annexation of Crimea and at the beginning of the aggression in Donbas [5,8,9]. In 2003, a modified version of the "Bide loop" was proposed by D. Brighton [10].

General Deptula D. further developed Warden's views and the content of 4GW wars. He planned to consider the enemy as a system at all national levels, including diplomatic, informational, economic, etc., and believed that non-military actions were an integral part of the new theory of conflict. As part of this, the United States created special teams to work in Iraq and Afghanistan, which included sociologists, ethnographers, linguists, and other specialists. These special groups communicated with the local population, influenced it, studied its habits, behavior, hierarchical structure, weaknesses and strengths of a particular social, ethnic and religious group, etc. In other words, they were actually forming an information base for conducting cognitive actions. In 2014, D. Deptula, together with J. Allen, presented a new concept of DIMET operations (DIMET: Diplomacy, Information, Military Power, Economy (including Finance) and Technology) at the conference "New US Military Strategy for a New Era", in which high technology is a key component [3],

For the first time, the system of conceptual presentation of the theory of network warfare with the definition of the role and place of information and other high-tech systems in it was presented in the publication "Network-Centric Warfare: Its Origin and Future" (August 1998) by Arthur Serebrowski and John Gorstka. Since the early 2000s, the United States has implemented the F3EAD (Find, Fix, Finish, Exploit, Analyze and Disseminate) cyber information cycle to improve the effectiveness of special operations forces. Its

implementation is aimed at gaining the ability to predict the enemy's actions, detect and determine the location and objectives of enemy forces. Central to the F3EAD process is the functional merger of intelligence and operations into a single process. These developments have not gone unnoticed in Russia.
In 2013, the Chief of the General Staff of the Russian Armed Forces, Valery Gerasimov, published an article with the eloquent title "The Value of Science in Prediction." Even then, anticipating the future actions of the aggressor state, he noted: "The emphasis of the methods of confrontation used is changing towards the widespread use of political, economic, informational, humanitarian and other non- military measures implemented with the use of the protest potential of the population. All of this is complemented by covert military measures, including the implementation of information warfare and the actions of special operations forces. The open use of force is often resorted to under the guise of peacekeeping and crisis management only at some stage, mainly to achieve final success in the conflict." [1]
It is interesting that Gerasimov did not mention (most likely deliberately) the main feature of the new war: its culmination takes place not on the battlefields, but primarily in the minds of people. The events of recent years in Ukraine show that the aggressor seeks not only to seize territory, but also to establish control over the worldview of millions of citizens of the country that has fallen victim to Russian aggression. The goal of this war (as planned) is to bring to a situation where the use of military force will become unnecessary, which is exactly what happened in Crimea. They needed people to betray their own country and support the aggressor. But it did not happen as expected.
General Gerasimov was, as it seemed, the storm-whisperer of the Kremlin's aggressive plans for a reason. At the time, it was not easy to see Ukraine as a potential target of Russian aggression.
All major theoretical studies and projects on the conduct of a new high-tech type of war clearly demonstrate that the key to victory in them is to ensure the achievement of information and technological superiority over the enemy and highly effective management. At the same time, information superiority implies the creation of systems for receiving, processing and analyzing information, reliable networks that connect troops and assets, enable them to exchange information and provide timely and complete overall situational awareness to commanders. Common situational awareness enables cooperation and self-synchronization, increases team resilience and speed, and in turn, increases mission effectiveness. The testing of such a distributed combat management information system FBCB2 (Force XXI Battle Command Brigade or Below), which covered the brigade-battalion-company level, took place in Iraq in 2013 [3,9]. At the same time, it is necessary to ensure the advance disabling and suppression of the enemy's intelligence and information support and control systems (intelligence means and systems, network-forming nodes, information and control centers).
According to Admiral W. Clark, "future operations will test revolutionary information technologies and the ability to disperse forces united by a single information space to achieve unprecedented offensive power, guaranteed defense and responsiveness in joint formations".
The essence of the NCW concept can be redefined as follows: it is a war of the "blind" against the "sighted". The physical strength of the "blind man" is the combat power of classical armed forces that do not take advantage of network-centric approaches, which does not guarantee an advantage in modern combat. This is a losing situation.
The NCW consists of 3 lattice subsystems: information, sensor (i.e., reconnaissance) and combat. But its basis is the information subsystem, whose goals, based on the concept, are the so-called Warden rings.
At the same time, the enemy's political technologies are conducting massive and coordinated information warfare operations aimed at demoralizing the population, creating panic and shock, and disorganizing the public administration system.
In this regard, the ratio of quantity and quality is viewed in a new light: you can have 90 or 550 brigades in the Army, but in the context of a war, when they are not ready for it, these brigades will not be able to perform combat missions.
Aggression using the principles of the NCW will consist of two stages.
At the first stage, high-precision air and space strikes will be carried out throughout the entire depths of the victim country's territory. Critical facilities will be targeted.

Lists of priority targets are drawn up in peacetime based on the concept of Warden's rings. By the way, this scheme was used in NATO's attack against Yugoslavia in 1999 and Russia's aggression against Ukraine in 2014 (annexation of Crimea and intervention in Donbas).

At the same time, the enemy will conduct massive and synchronized information warfare operations:

- psychological operations;
- electronic suppression and destruction of the system of state, economic, financial and military management, communications, intelligence and electronic warfare;
- offensive computer operations (cyber warfare);

The purpose of the first stage of aggression will be:

- disorganization of the system of state, economic, and military governance;
- demoralization of the population, panic and shock;
- disorganization of the victim's country's military activities;
- "blinding" the victim's intelligence and air defense system.

The second stage of aggression is a ground invasion, which begins only when the goal of the first stage is achieved and when it is deemed necessary. In essence, it will be a cleansing of the area.

A characteristic feature of the second stage of aggression will be that the enemy's troop groups will not conduct classical warfare. The very possibility of enemy groups engaging in combat will be excluded. Characteristic features of this stage of aggression:

- the enemy will be ahead of the victim state at all stages: collecting and evaluating information, making decisions and actions;
- there will be no concentration of troops, withdrawal of troops, deployment in combat order, direct attack, pursuit or retreat to new lines;
- there will be no borders, no stripes, no flanks, no fronts and no rear;
- the enemy will have absolute information dominance on the battlefield - every soldier of the victim country will be visible;
- the rigid hierarchical system of military command will be replaced by a flexible network system, subordinate troops will be free to choose their methods of action, and the organizational and staffing structure of the troops will be constantly changing to adapt to the requirements of the situation;
- widespread use of tactical ground and aerial robotic systems that will operate in the rear, destroying centers of resistance.

All this radically changes the idea of war, taking it beyond the physical sphere into the information sphere. Contactless warfare is becoming a reality. And here the experience of the Second World War in organizing and conducting strategic offensive operations can become dangerous and also harmful.

There is also a psychological component to the NCW concept: those who actively use the benefits of network-centered approaches develop absolute self- confidence. The threat to the life of a particular soldier on the battlefield becomes minimal. Military operations turn from a life-and-death struggle into a computer game based on the principle: "I can see you, but you can't see me". This, according to the authors of the concept, should lead to disorganization and demoralization of the opposing side's personnel even before entering the battle. The party that does not take advantage of the NCW will lose control in a short time and will ultimately be defeated.

NCW is neither a myth nor a fantasy. Experts believe that the concept of NCW is universal and can be used to combat any type of enemy: regular and irregular troops, modern and traditional.

It should be noted that NCW has special properties compared to traditional warfare [11]:

1. The broad power of using a geographically distributed force. Previously, due to various limitations, it was necessary for units and logistics elements to be located in one area in close proximity to the enemy or the defended object.
2. The second difference between the NCW is that the forces participating in it are highly intelligent: using the knowledge gained from a comprehensive view of the battlespace and a situated view of commanders' intentions, these forces will be able to self-synchronize their activities and become effective in autonomous operations.

3. The third difference is the existence of effective communications between objects in the combat space. This allows geographically distributed systems to conduct joint operations, as well as dynamically distribute responsibility and the entire workload to adapt to the situation. As a result, the total bandwidth of the satellite communication channels leased by the Pentagon for information transmission has increased more than seven times since 1991.

NCW is aimed at converting the information advantages inherent in individual information technologies into a specific advantage by combining them into a stable network of information-rich, geographically dispersed forces. This network, combined with known technologies, organization of processes and people, allows the use of new forms of warfare.

Based on this, we formulate the principles of conducting NCW

1. Forces connected by reliable networks can improve information sharing.
2. Information sharing improves the quality of information and overall situational awareness.
3. General situational awareness allows for cooperation and self- synchronization, increases team resilience and speed.
4. This, in turn, increases the efficiency of the operation.

Taking into account the peculiarities of the NCW in relation to any theater of war, the concept of this war envisages 4 main phases of warfare:

1. Achieving information superiority through the preemptive destruction (disabling, suppression) of the enemy's intelligence and information support system.
2. Gaining air superiority by suppressing enemy air defense systems.
3. Gradual destruction of protected control and information bases of enemy combat equipment, primarily missile systems, aircraft, artillery, and armored vehicles.
4. Final destruction or suppression of enemy resistance centers.

The successful implementation of each phase is based on a much shorter duration of the combat cycle "detection-recognition-destruction" in relation to the enemy, on direct and complete information about the enemy's grouping.

In military terms, NCW allows us to move from war of attrition to a shorter and more effective form, which is characterized by two main characteristics: speed of control and the principle of self-synchronization.

The speed of management in the view of experts has the following aspects:

1. The troops achieve information superiority, which does not mean receiving large amounts of information, but higher degrees of representation and a deeper understanding of the situation on the battlefield. In technological terms, all this implies the introduction of new command, control, intelligence, and computer modeling systems.
2. Troops with information superiority implement the principles of disguising results rather than disguising forces.
3. As a result of such actions, the enemy loses the ability to pursue any course of action and falls into a state of shock.

The principle of self-synchronization came from the theory of complex systems. According to this theory, complex phenomena and structures are best organized in a bottom-up manner.

In other words, by self-synchronization, experts understand the ability of a military structure to self-synchronize from below, rather than change in accordance with instructions from above. The organizational structure of units and subunits, norms and methods of performing combat missions will be modified by the decision of the commander on the battlefield, but in accordance with the needs of the higher command.

This principle contradicts the traditional foundations of a centralized hierarchical military organization, which is based on subordination to directives from the top. It is difficult to break such a system, as it requires changes not only in organizational forms and methods of management, but also in the mentality of superiors and subordinates. However, the principle of self-synchronization has already been implemented by the Ukrainian armed forces.

The use of self-synchronization systems allows you to achieve an advantage over the enemy in the speed and suddenness of actions. Tactical and operational pauses that the enemy could take advantage of disappear, and all management processes and combat operations themselves become more dynamic, active

and effective. Military operations are no longer taking the form of successive battles and operations with appropriate pauses between them, but rather continuous high-speed actions with decisive goals.

On the basis of these principles and phases of NCW in Ukraine, a system of ensuring Ukraine's military security was formulated, which is related to both external and internal spheres of the state's activity. The external aspect is to stabilize the military-political situation in the region and in the world, to reduce the level of military threat to Ukraine from other states, primarily from Russia. The internal sphere covers issues related to solving socio-economic problems, maintaining the state's defense capability, including the combat potential of the Armed Forces, mobilization capabilities, etc.

The basis for ensuring military security of Ukraine as a non-nuclear state is based on three basic concepts. First, it is the concept of military-political partnership based on a developed economy with rational infrastructure, a stable sphere and a sound military policy aimed at increasing strategic stability in the region and reducing the level of military danger by political and economic means.

Secondly, it is the concept of defensive deterrence, whereby a military organization of the state is created in networks of defensive expediency, which is able to minimize the likelihood of a military conflict by threatening to inflict unacceptable damage on a possible aggressor, as a result of which he loses the incentive to attack.

Thirdly, it is the concept of repelling possible aggression, which is based on mobilizing all the country's capabilities and resources to counter a military attack, defeat the aggressor, and suppress it until hostilities cease. But this security system did not work as it was formulated in peacetime.

The main content of ensuring Ukraine's military security is in peacetime in a threatening period with the beginning of repulsing armed aggression. At present, we are more interested in repelling the aggression that Russia has committed against Ukraine [13]:

- timely introduction of martial law or a state of emergency in Ukraine or in some of its regions, full or partial strategic deployment of the Armed Forces of Ukraine, bringing them and other military formations to readiness to perform the tasks of localizing a military conflict and repelling armed aggression;
- transferring Ukraine's national economy, enterprises, transportation and communications to martial law;
- deployment of strategic command and control systems of the Armed Forces of Ukraine and other military formations, operational, logistical, technical and medical support systems, as well as forces and means of territorial and civil defense, in accordance with the requirements of wartime;
- concentration of efforts of state authorities and military authorities, local self-government bodies, public organizations and citizens on fulfilling the tasks of state defense;
- full use of the capabilities of international security organizations to stop a military conflict, localize it and prevent it from escalating into a local (regional) war;
- repulsing an armed attack, striking at the aggressor's troops and most important targets in order to force it to abandon further (combat) operations at the initial stage of armed aggression and to conclude peace on terms that meet the national interests of Ukraine.

For Ukraine's defense, the concept, content, and characteristics of the threatening period were extremely important. Ukraine's efforts in the field of defense, as well as the principles of negotiating and concluding agreements on military and political issues, were aimed at ensuring conditions under which Russia's attempted aggression against Ukraine was not felt and this period was to be longer. This would have allowed Ukraine to solve its defense problems, given that the Armed Forces of Ukraine had a smaller number of troops [12,13].

The results of the analysis of a possible war for Ukraine and the assessment of the state of Ukraine's military security in 2010 made it possible to identify the following main ways to improve the preparation of the state's defense in the interests of increasing the threat of a military conflict:

1. Create an effective early warning system for military threats.

The basis of such a system was to be formed by the information capabilities of the General Staff of the Armed Forces, the Security Service of Ukraine, the Border Troops, the intelligence forces of the Armed

Forces and the operational command headquarters. First of all, this concerns the intelligence channels of agents, radio and radio-technical channels. Combined into a single system under the direct supervision of the General Staff of the Armed Forces of Ukraine, these forces and means can provide reliable and timely information on signs of the enemy's preparation for aggression and the probable timing of the beginning of hostilities with the pre-emptive action necessary for the appropriate deployment of troops and other preparations to repel aggression.

2. Refusal to keep a significant number of discharged units and formations in the Armed Forces and other peacetime military formations. It is advisable to have well-equipped and fully combat-ready units and formations that can repel aggression in case of aggression. In this case, a potential enemy will not be able to hope for the success of a sudden military attack without prior deployment of its armed forces.

3. Increased attention to the protection of the most important groups of troops and facilities from air strikes. This also reduces the likelihood of a surprise military attack on Ukraine.

4. Increased attention to the country's advance preparation for war, especially its operational organization. This will also force a potential aggressor to increase the volume of preparations for an armed attack, thus losing time and the factor of surprise.

However, these tasks were not fulfilled because in early 2013 nothing boded well for Yanukovych's resignation. The Verkhovna Rada was dominated by a presidential majority based on the Party of Regions, which easily bent the legislative process to its own advantage. Ukraine looked completely controlled and submissive to Russia, and nothing portended large-scale social upheaval, let alone military aggression. Gerasimov had not yet made a speech on the future actions of the Russian leadership, although they were already being planned.

The annexation of Crimea was planned by the Russian Federation in accordance with Gerasimov's views and the systemic model of the NCW based on Warden's theory. As already noted, an object with critical cyber infrastructure is a center of gravity according to Warden - the point where the object or subject of influence is most vulnerable [4, 5, 8].

Warden's model is implemented according to the "war from the middle zone" scheme. It should be noted that this model works well in conflict zones where the armed forces are viewed by the local population as an external aggressor.

In contrast to this model, Russia has long had support from the local population and significant military formations of the Black Sea Fleet in Crimea, which were not perceived as an aggressor or enemy [8,9].

Russia had a long preliminary influence on the population of Crimea in order to perceive the military of the Russian Federation as defenders of the population and to correct the "historical mistake" of subordination of Crimea to Ukraine. Then, the influence on the leadership of the Autonomous Republic of Crimea and the city of Sevastopol began, followed by information and psychological influence (according to the theory of NCW) on the personnel of the Armed Forces of Ukraine. The main objects of transport infrastructure and life support systems were taken under control. Russia's actions during the campaign to bring its Armed Forces into Crimea were accompanied by actions that bore all the signs of a prepared and thoughtful operation in terms of goals, measures and consequences, aimed primarily at the Russian community, and on the other hand, at Ukrainian and Western society.

The tactics of hybrid warfare used by Russia in Crimea were, with certain changes, used in Donbas. During the aggression in the southeastern region of Ukraine, the main impact was focused on the population of the region, followed by the state infrastructure and life support system, respectively. The fourth and fifth objects of influence were the Armed Forces and military and political leadership of Ukraine.

The peculiarity of Russia's hybrid war in Donbas and Ukraine at that time was and still is the constant search for and use of relevant information triggers that can form the necessary public opinion. There was also a tendency (expansion) of the outpouring to areas that were previously not typical for information confrontation, namely, the revision of the history of statehood of Ukraine and Russia and interfaith relations.

In order to achieve Russia's political goals and destabilize the situation, terrorist acts carried out by sabotage and reconnaissance groups not only in the Joint Forces Operation area (formerly the Anti-Terrorist

Operation) but also in other regions of Ukraine have become widespread. The aim was to intimidate the population and reduce the moral and psychological state of the personnel of the Joint Forces Operation units. Illegal armed groups used demonstrative and provocative hostilities.

It should be noted that the war in cyberspace began on February 14, 2022. On that day, Russian hackers launched a powerful cyberattack on Ukrainian government agencies and the banking system. From that day on, constant cyberattacks on Ukrainian systems began. And on February 24, 2022, Russia launched a special operation against Ukraine, i.e. a large-scale aggression against a sovereign state. It should be noted that the hybrid war has reached a new level. In addition, the Russian media emphasized the defense of the Luhansk and Donetsk People's Republics from Ukraine's attack, denazification and demilitarization of Ukraine, and most importantly, the protection of the Russian-speaking population of Ukrainian society.

It should also be noted that on the night of February 23-24 (in accordance with the NCW concept), Russian hacker groups carried out a number of additional cyberattacks on the websites of Ukrainian government agencies and media.

These actions are similar to the actions of the Russian aggressor in the war with Georgia in 2008[9], when they launched cyberattacks on Georgian government websites before the aggression. However, Ukraine's cyber defense worked well, which made it possible to protect most sites.

According to Russian plans, which were announced in their media, they were supposed to capture Kyiv in 3 days and completely occupy Ukraine in 9 days. But it did not happen as expected.

It should be noted that the most important from the point of view of the theory of military strategy is the initial period of war (IPW). It is understood as a period of hostilities when the opposing parties, carrying out the first operations of the armed forces in the form of created groups of troops and forces, act in accordance with pre- developed plans, try to seize the strategic initiative, inflict maximum losses on the enemy and create favorable conditions for achieving the goals of the war [12].

This general definition can be extended to the concept of the IPW for Ukraine.

The study of the NCW experience suggests that the following are characteristic of the IPW [1, 14]:

- high tension and dynamics of the fighting;
- a decisive struggle for air dominance and firepower;
- uncertainty of the situation and the speed of its change;
- simultaneous action by fire and strike forces, airborne troops to the full depth of the enemy's operational structure with concentration of main efforts on the main directions and most important objects;
- massive use of reconnaissance and sabotage groups, airborne and airborne troops;
- increasing the role of all types of intelligence and covert command and control of troops;
- the dependence of the success of combat operations of troops on the comprehensiveness and level of their operational and combat training.

The specific goals of Russia's war against Ukraine are the elimination or change of the existing political system, deprivation of sovereignty and territorial integrity, etc.

Based on this, the aggressor used various forms of warfare during the IPW, including terrorist, sabotage, information, etc.

Since the most important defining feature of the IPW is the struggle for strategic initiative, it can be divided into the following two phases:

- first, the phases of fire and other mutual actions of the groups of troops of the parties in order to create conditions for seizing air dominance and achieving fire superiority, raising the moral and psychological state of special forces and the population;
- second, the phase of using the results of defeating the enemy and acting on it by defeating its strike groups, capturing key frontiers in order to seize the strategic initiative.

Analyzing the phases of the IPW, we can conclude that Ukraine won this stage of the war. At the beginning of Russia's war against Ukraine, the situation was very difficult. The aggressor approached Kyiv and Kharkiv, captured Kherson and part of Zaporizhzhia region, and dug in Chernihiv and Sumy regions. However, in March 2022, the Armed Forces of Ukraine managed to drive the enemy back from Kyiv and

Kharkiv, and then liberate Chernihiv and Sumy regions. The defense forces were able to turn the tide of hostilities. The Russians failed to achieve air superiority in the full sense of the word. They could not break the morale of our soldiers and civilians, but only strengthened it. They also failed to capture key pipelines. On the contrary, in September-October, the Ukrainian Armed Forces liberated Kharkiv region and then Kherson. Therefore, it can be argued that the Russians have lost the IPW.

Modern warfare in terms of methods and means of conduct is significantly different from that of the mid-20th century. Ukraine, with the help of its Western partners, has mastered this, while Russia fights as it did in World War II. Ukraine uses:

- transition from command and control of troops and weapons to management of armed struggle;
- formation and use of situational reconnaissance and strike systems in combat zones, which combine existing intelligence and control systems and means of communication into a single system;
- transfer of the main load of actions to the information-cybernetic, cognitive space;
- informational, psychological, cognitive, cybernetic actions become an integral and predominant component of military actions;
- accessibility to all elements of the battle space for all combatants;
- large-scale, systematic use of innovative high-tech weapons and military equipment, hypersonic, high-precision and guided weapons;
- conducting combat operations remotely (if possible);
- robotization of armed struggle;
- increasing the role and expanding the use of special operations forces and cyber forces;
- growing asymmetry in the nature of hostilities.

At the same time, Russia is fighting only with the number of troops, not with equipment. And at the same time, it is suffering very large human losses.

It should be noted that Russian propaganda plays an important role.

Just look at the current Russian-Ukrainian war. At the beginning of the full- scale invasion, Russian propaganda shouted: "Kyiv in three days", "Kyiv capture in the morning, and a parade on Khreshchatyk in the evening", and so on.

The invaders were sure that Ukrainians would welcome them as liberators and with flowers, and were surprised to see the fierce resistance of Ukrainians.

If you recall history, before the battle for Grozny (1994), Russian General Grachev said that he needed two hours and one parachute regiment to take the Chechen capital. But two days later, the Chechens burned all the Russian tanks and armored personnel carriers that had entered Grozny, and the Russians were partially killed or captured.

The biggest disadvantage of the Russian army is its underestimation of the enemy. In every war, for some reason, the Russians were confident that they would win very easily. For example, even before the outbreak of World War II in 1938- 1939, the Soviet command assured that the war would be fought on foreign territory, that the Union would fight with "little blood," that the Soviet Union's opponents would not be able to resist with dignity because they did not have an equally "powerful" army.

The army of any country in the world has its own traditions, which have been formed over centuries. The modern Russian army considers itself the successor to the Soviet army and partly to the tsarist army. For all three armies, the nature of officer training and warfare has hardly changed in more than 100 years.

According to experts, Russians are very self-confident. Their favorite phrase is "We are Russians. God is with us!" Therefore, they believe that they simply cannot lose the war. It is a kind of ego boosting.

In general, Russians are very fond of appealing to past victories. For some reason, however, they do not mention that those were the days of the Russian Empire or the Soviet Union, and not only Russians fought.

CONCLUSION

It should be noted that in modern conditions, the nature of the information-military struggle has changed significantly: it is increasingly taking on the characteristics of a hybrid war. The emphasis of the military

struggle is shifting towards the practical implementation of information technologies. At the same time, informational and psychological operations, actions and actions are gaining more and more importance in achieving political and military goals.

It should also be noted that this article was prepared in November 2021. However, on February 24, 2022, Russia's war against Ukraine began. Therefore, it one should state that some conclusions and provisions of the article have been confirmed in life.

BIBLIOGRAPHY

1. Magda E. Russia's Hybrid Aggression: Lessons for Europe - K: KALAMAR Publishing House, 2017. - 268 p.
2. Permyakov O.Yu., Zbitnev A.I. Information technologies and modern armed struggle - Luhansk: Znannya, 2008. 204 p.
3. Danik Y.G. High-tech aspects of ensuring national security and defense
4. // Communications and Networks. Telecom. 2018, October, special issue. pp. 58 - 69.
5. Pirtskhalava L.G., Khoroshko V.A., Khokhlacheva Y.E., Shelest M.E. Information and analytical security support - K: FOP Yanchinsky A.V., 2021.-470p.
6. Grishchuk R.V., Danik Y.G. Fundamentals of cyber security - Zhytomyr: ZhNAEU, 2016. - 636 p.
7. World Hybrid War: Ukrainian Front / Edited by V.P. Horbulin - L: NISS, 2017. - 496 p.
8. Samoilov I.V., Konotov O.V., The concept of Byz, Communications and Networks. Telecom, 2016, September, special issue. pp. 66 - 67.
9. Pevtsov G.V., Zalkin S.V., Sidenko S.O., Khudarkovsky K.I. Information and Psychological Operations of the Russian Federation in Ukraine: Models of Influence and Directions of Counteraction // Science and Defense. № 2. 2015. - c. 28 - 32.
10. Artemov V., Khoroshko V., Brailovsky M., Khokhlachova Y., Pirtskhalava T. Methoods of Preparing and Conducting Modern Hybrid Wars // SPCSI, v. 6, no. 3. 2022. - p. - 1 - 12.
11. Bryant D. I. Critique, Compare and Adapt: A New Model of Command Decisionmaking. Defend R&D Toronto Technical Repost, DFDC, Toronto TR, 2003. - 63.
12. Biriukov V.O., Esaulov M.Y., Zhuk P.V., Minochkin A.I., Pavlov I.M. Theoretical foundations of information warfare in modern wars, military conflicts and wars of the future - K: VITI DUT, 2013. - 322
13. Boriskin V.D., Military-political and military-strategic assessment of the possibility and nature of local wars and conflicts for Ukraine // Nauka i oborona, No. 1, 1995, pp. 52-56.
14. Shkidchenko V.P., Kokhno V.D. Elements of the theory of military security - K: Charitable Foundation "Peacemaker", 2001. - 194 p.
15. Khoroshko V., Khokhlachova Y., Ivanchenko I., Pirtskhalava T. Information weapons as an instrument of information warfare // Information Protection, Vol. 24, No. 2, 2022. pp. 50 - 85.
16. Tolubko V.B. Information warfare: conceptual, theoretical, technological aspects - K: NAOU, 2003.320 p.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 65 – 73 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

LEADING THE WAY IN QUANTUM-RESISTANT CRYPTOGRAPHY FOR EVERYDAY SAFETY

Luka Baklaga[1]
[1]Research and Development Department, Business and Technology University, Georgia

ABSTRACT: The development of quantum-resistant solutions is imperative as the emergence of quantum computing presents a substantial risk to existing cryptography systems. Lattice-based cryptography, especially schemes based on the Learning with Errors (LWE) problem, is one of the most promising methods. To guarantee long-term security, even LWE-based methods could need to be strengthened further as quantum algorithms advance. By mixing Gaussian and discrete uniform distributions to create a mixed error distribution, this work enhances the classic LWE problem. The experimental findings show that, with a slight rise in computing overhead, the mixed error distribution improves the security of the LWE problem by strengthening its resistance to quantum techniques. By presenting a novel approach for enhancing the resilience of cryptographic methods in the quantum era, this research contributes to the continuing work in post-quantum cryptography. Moreover, it introduces the direction of future model improvements and provides multidisciplinary methods for increasing the complexity of cryptographic algorithms.

KEYWORDS*:* Post-quantum cryptography, Lattice-based cryptography, cryptography, quantum-resistant, PWE, Gram-Schmidt Orthogonalization, quantum security

1. INTRODUCTION

The need for quantum-resistant cryptography systems is growing as quantum computing comes forward to being used in everyday applications. The difficulty of key search operations can be greatly reduced by quantum computers, lowering the level of security of symmetric cryptosystems. A class of technologies known as "quantum computing" aims to accelerate processing by utilizing quantum effects like superposition. The implicit computation of several values at once is made possible by superposition. Because of the mode of computation, tiny qubit sized quantum computers are exponentially faster than classical supercomputers. Search, hidden subgroups, and quantum simulation are the three main problem classes in which quantum computers can perform better than classical computers (Hasan et al. 2024). In the current cryptographic landscape, there are two primary types of cryptography: symmetric and asymmetric. The effectiveness of symmetric and asymmetric algorithms varies significantly based on several parameters, including security threats, latency, and key size. One prominent symmetric algorithm is the Advanced Encryption Standard (AES). AES is a symmetric block cipher that operates with different block sizes and supports key lengths of 128, 192, and 256 bits. In contrast, the Data Encryption Standard (DES) processes 64 bits of plaintext to produce 64 bits of ciphertext. This operation involves substitution and permutation through a series of rounds, with decryption performed in reverse. However, 64 bits is considered insufficient for secure environments, making it relatively easy to break. As a result, the Triple Data Encryption Standard (3DES) was developed as an enhancement to DES. Another symmetric algorithm is Blowfish, which utilizes a variable-length block cipher with key lengths ranging from 32 to 448 bits. On the other hand, there are mathematically complex asymmetric algorithms. One well-known algorithm is RSA, a public key cryptosystem where one key is shared publicly while the other key remains private and secret. Elliptic Curve Cryptography (ECC) has emerged as a promising alternative, particularly in cryptographic applications, due to its efficiency in addressing the logarithm problem in finite fields. While ECC and RSA are similar, they differ in that ECC uses a different cryptographic algorithm and has a faster solution capacity. Since discrete logarithms and integer factorization are mathematical challenges, traditional encryption protocols like RSA and ECC are projected to be easily cracked by quantum algorithms like Shor's algorithm. The factoring number problem can be solved in polynomial time using

Shor's technique, whereas the best classical solution (General Number Field Sieve) required exponential time to solve previously (Bavdekar et al. 2023). Therefore, to avoid this catastrophe, the National Institute of Standards and Technology (NIST) has initiated steps to standardize post-quantum cryptography (PQC) primitives that implement at least one of the following functionalities: public key encryption, key encapsulation mechanism (KEM), or digital signature. This initiative is designed so that participants can submit their algorithms and then compete against each other's entries for a few years. After then, NIST selects a winner based on suggestions from the cryptography community (Schneier 2022). Consequently, post-quantum algorithms are a method for developing quantum secure cryptography. Post-quantum algorithms are dependent on a variety of different mathematical fields and issues, such as multivariate cryptography, hash-based cryptography, code-based cryptography, and lattice-based encryption, whose mathematics is both more difficult and less understood (Bernstein, Buchmann, and Dahmen 2009). The Learning with Errors (LWE) problem is one of the most researched lattice-based encryption challenges, and it serves as the foundation for several proposed quantum-resistant cryptographic algorithms. The security of the LWE problem derives from the fact that noisy linear equations over finite fields are inherently hard to solve, even for quantum computers. Nonetheless, there is still a need to strengthen the security of LWE-based systems as quantum computing advances. This study introduces a mixed error distribution as an improvement to the classical LWE problem. The proposed method combines Gaussian and discrete uniform distributions to increase the unpredictability of the error vector, potentially improving the security against both classical and quantum attacks, while previous work has concentrated on specific types of error distributions, usually spherical Gaussian noise. This study's main objective is to assess the trade-offs between performance and security that come with this mixed error distribution. This work intends to add to the expanding corpus of research focused on fortifying cryptographic systems against the impending threat of quantum computers, ensuring the security of routine digital communications, by investigating a new avenue in LWE-based encryption. The article also tries to demonstrate fresh potential avenues for model improvement and the reasons an interdisciplinary approach would be advantageous for safeguarding our digital environment in the future. As a result, we have the chance to plan how to switch out the outdated algorithms with post-quantum ones as they become available. Give top priority to the systems that transfer or store your most sensitive information and determining which mathematical technique or post-quantum algorithm is most likely to be successful against qubit-based attacks.

2. OBJECTIVES

By adding a mixed error distribution, the primary objective of this study is to analyze, simulate, and improve the Learning with Errors (LWE) problem, which is a fundamental component of lattice-based cryptography. In previous instances, LWE has secured cryptographic systems with Gaussian noise. Stronger security measures are, nevertheless, required due to the growing threat posed by quantum computing. In this study, we propose a simulation based on experimental results and equations derived from prior research. Furthermore, we introduce a novel approach that integrates Gaussian and discrete uniform noise to generate a complex, intricate, and unpredictable error distribution. Our objectives are to evaluate performance, conduct a trade-off analysis of various models, and provide conclusive validation. In order to support quantum-resistant cryptography without substantially sacrificing computing efficiency, this study aims to bring light on the possibility of mixed error distributions.

3. RESEARCH METHODOLOGY

3.1 PROBLEM DEFINITION

The paper's experimental structure begins with an analysis of the previously published paper "Quantum-Resistant Lattice-Based Cryptography : New Conjectures on the Learning with Errors Problem, which primarily focuses on the Learning with Errors (LWE) problem (Baklaga 2024a, 50–56). This problem forms the foundation of various lattice-based cryptographic schemes. Based on experimental results

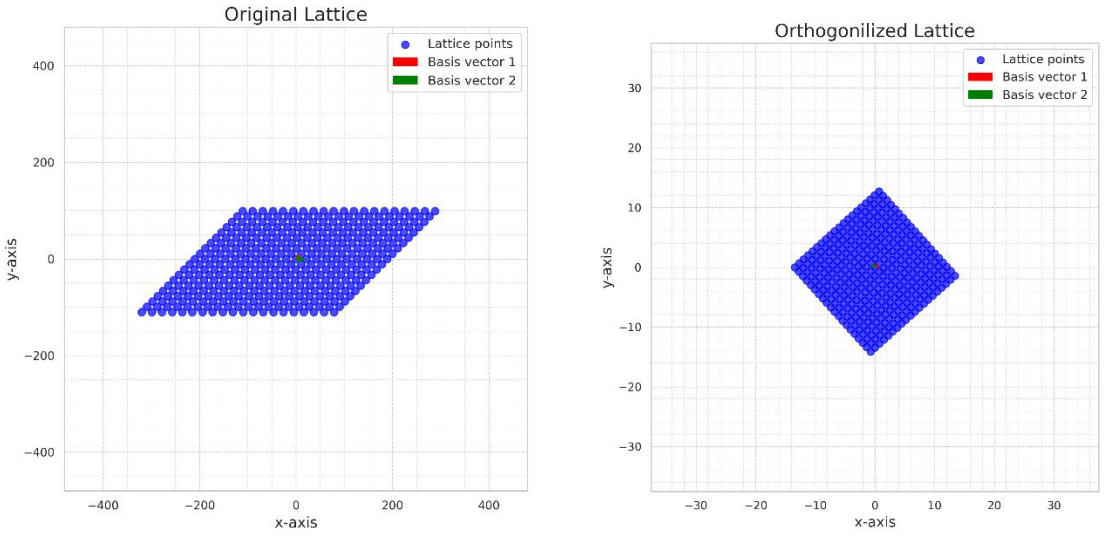
and proposed equations, we have developed scientifically accurate simulations of the mathematical models, including the LWE problem, GapSVP, and SIVP, under the various error distributions outlined in the original paper.

The simulation structure initially involves modeling the configuration of an n-dimensional lattice using basis vectors $B = \{b_{1,\dots,}b_n\}$. Discrete Gaussian sampling is employed to generate error distributions, as described in the paper. Consequently, the lattice Λ is defined as follows:

$$\Lambda(B) = \left\{ \sum_{i=1}^{n} z_i b_i : z_i \in \mathbb{Z} \right\}$$

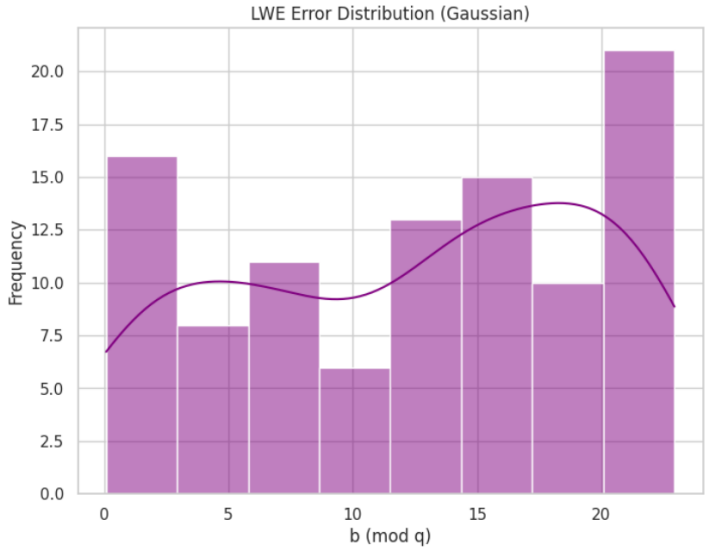
A model has been implemented that generates Learning With Errors (LWE) samples. Simulations of the Gap Shortest Vector Problem (GapSVP) and the Shortest Vector Problem (SIVP) have been created, with the goal of approximating the shortest vector in a lattice. As described in the paper regarding Conjecture 4.1, this can be modeled by embedding lattice structures into higher-dimensional spaces and solving for the shortest vector using LWE-based reduction techniques. For Conjecture 4.2, the paper suggests a quantum reduction from GapSVP to LWE using spherical errors. Consequently, we have simulated a quantum oracle-based approach to demonstrate the quantum security assumptions made by LWE. Finally, we have validated the theoretical claims by running simulations across varying lattice dimensions n, modulus q, and error distribution parameters $\sigma, b, \beta_1, \beta_2$. We also considered optimizing the implementation by parallelizing parts of the computation due to the complexity of large-scale lattice reductions. Therefore, we utilized algorithms such as Gram-Schmidt Orthogonalization on high-dimensional lattices. In the Google Colab environment, various libraries have been utilized, including NumPy for matrix and mathematical operations related to random sampling, Matplotlib for the precise generation of plots based on simulation output, SciPy for mathematical operations on norms and vector distances, and finally, SymPy for implementing the Gram-Schmidt Orthogonalization lattice reduction algorithm. As part of the experimental procedure outlined above, the libraries have been installed. We will first generate a basis and perform a reduction using the Gram-Schmidt Orthogonalization algorithm, which is one of the primary and easily implemented algorithms in lattice-based cryptography. The Gram-Schmidt Orthogonalization algorithm is employed to find short, nearly orthogonal vectors in a lattice.

***Fig.1**. Vectors in a lattice (Lattice Generation)*



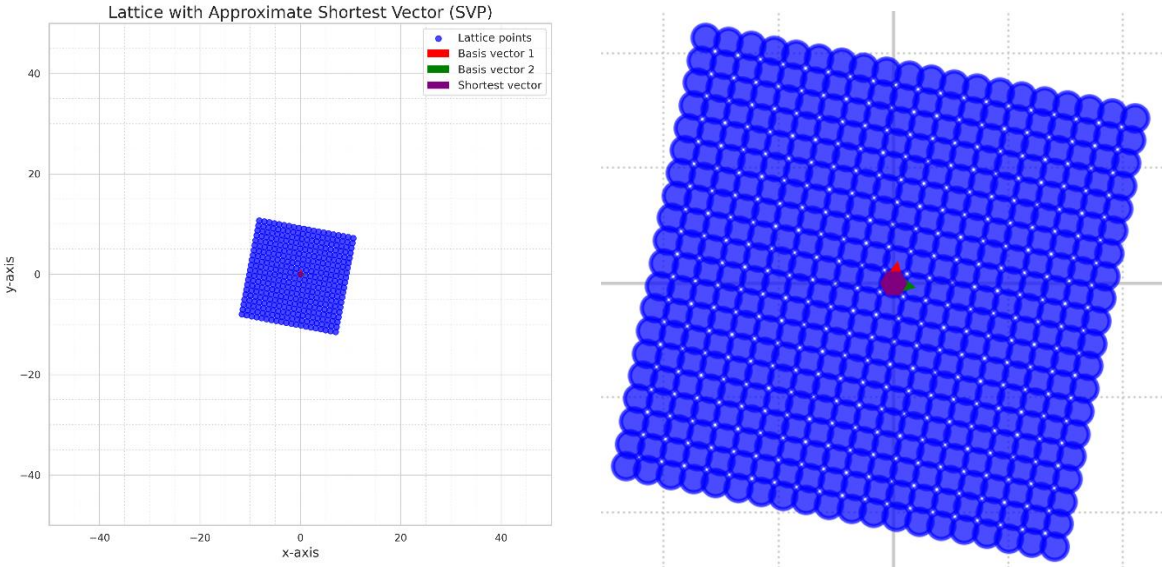
As the second part of the simulation, the Learning With Errors (LWE) problem generates random samples from a secret vector *s* combined with Gaussian noise. Therefore, from this perspective, we simulate the problem using a secret vector to create visualizations of the distribution.

***Fig.2**. LWE simulation (Error distribution point)*



From the experimental steps, the Gaussian error generated by the code is sampled using "np.random.normal()". We visualize the distribution using a histogram with a kernel density estimate (KDE) to illustrate how the errors are distributed.
Finally, to approximate the Shortest Vector Problem (SVP), we apply the Gram-Schmidt Orthogonalization algorithm to the lattice and visualize the shortest vector.

***Fig.3**. LWE Visualizing GapSVP Approximation*



This Python-based cloud simulation offers a mathematically rigorous and visually rich framework for simulating lattice-based cryptography using necessary libraries. As demonstrated in this paper, we have simulated lattice generation and reduction using the Gram-Schmidt Orthogonalization algorithm.

Additionally, there are more effective algorithms, such as LLL and HNF,that provide improved accuracy and visualization. We have also presented the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP) solution through lattice reduction.

3.2 ENHANCED LWE DEFINITION

A fundamental obstacle in lattice-based cryptography, the Learning with Errors (LWE) problem is generally considered a strong contender for post-quantum cryptographic algorithms. Traditionally, the LWE problem uses a Gaussian error distribution, which introduces noise into the linear equations obtained from a secret vector to guarantee that the challenge stays hard (Baklaga 2024a, 50–56). Because of this noise, recovering the secret vector is computationally impossible, protecting the cryptosystem from intrusions. But much more robust defenses are now required due to the advent of quantum computing. This work introduces a mixed error distribution as an improvement to the LWE problem. In contrast to the conventional method that exclusively uses a Gaussian distribution, this novel approach introduces a dual-layered complexity in the error vector by combining a discrete uniform distribution with a Gaussian distribution.

Firstly, the foundations of the Gaussian distribution (narrow examination as Gaussian Kernel), commonly referred to as the normal distribution, have been introduced. The Gaussian distribution (GD) is typically characterized by its bell-shaped curve and is mathematically defined as follows:

$$\rho_\sigma(x) = \exp\left(-\frac{\pi\|x\|^2}{\sigma^2}\right)$$

The spread of the distribution is controlled by σ, which in this case stands for the standard deviation on the model. Within the framework of LWE, Gaussian noise offers a consistently demanding error term that makes it more difficult to recover the secret vector s. However, in addition to the first model, there also has been presented the discrete uniform distribution, which was characterized by an equal likelihood for any value falling inside a given metric range. As an illustration, we can identify the integer range$[-a, a]$, in which case the probability mass function is as follows:

$$P(X = x) = \frac{1}{2a+1}, x \in \{-a, -a+1, \dots, a\}$$

We may infer from this distribution that Gaussian noise would be more predictable than randomly supplied unpredictability, providing an extra line of defense against random attacks that might take advantage of the Gaussian distribution's smoothness. By merging these two distributions and examining suggested distribution models, we can improve the LWE problem. By doing so, we can add a new error vector called e_{mixed} , which is expressed as follows:

$$e_{\text{mixed}} = \left(e_{\text{gaussian}} + e_{\text{uniform}}\right) mod q$$

Where, the Gaussian distribution itself is used to sample e_{gaussian} from the equation, and the discrete uniform distribution is used to sample e_{uniform} .

The equation displays a dual-distribution approach model, which, in addition to the regular distribution strategy, produces an unpredictable point complex noise structure and a higher uncertainty metric, making the task harder. With all of the previously listed features, this idea offers more defense against attacks based on quantum computation.

The primary objective of the proposed experiment is to evaluate and compare the security and efficiency of the traditional Learning with Errors (LWE) problem, which utilizes Gaussian noise, against the enhanced LWE problem that incorporates a mixed distribution of Gaussian and uniform noise. The evaluation will focus on key performance metrics, including encryption and decryption times, resistance to attack simulations, and overall computational efficiency. These metrics are essential for assessing cryptographic security and will be applicable for future deployment. For the experiment involving

modeling and simulation based on the proposed mathematical equations, we have utilized various tools and environments. The experiment will be conducted using Python in the Google Colab cloud environment. This environment has been chosen to leverage high-performance computing capabilities, allowing us to effectively manage the computational load associated with large dimensions. Python was selected due to its extensive range of open-source libraries; specifically, we will leverage the NumPy and SciPy libraries for numerical operations and distribution sampling within the model. These libraries are designed to meet the mathematical demands of the Learning with Errors (LWE) problem, providing efficient implementations of linear algebra and random functions. For the implementation of the algorithm, we developed a series of steps for the Learning With Errors (LWE) problem, which will utilize a Gaussian error distribution. Our objective is to establish a baseline for comparison; therefore, the focus will be on simulating the standard formulation of LWE. Subsequently, the enhanced LWE problem will be implemented using a mixed error distribution. The advanced version of this hard problem will combine Gaussian noise with discrete uniform noise, aiming to evaluate the impact on security and computational overhead.
Simulation parameters are defined as random variables that can be tested with different values to reduce the probability of random noise and to identify the average output. For this simulation, the parameters are represented as follows:

- n = 50: Dimension of the secret vector s
- q = 101: A prime modulus representing the field $\mathbb{Z}_q$
- m = 60: Number of samples generated for the LWE instance,
- σ = 3.0: Standard deviation for the Gaussian noise distribution
- $uniform\_scale$ = 5: Range for the uniform distribution

The algorithm implementation began with the traditional Learning With Errors (LWE) problem, which is based on Gaussian noise. In this traditional problem, noise is sampled from distributions, most accurately from a Gaussian distribution. Therefore, the matrix $A \in \mathbb{Z}_q^{m \times n}$ is generated randomly, and the error vector e_{gaussian} is sampled from a Gaussian distribution.

$$e_{\text{gaussian}} \sim \mathcal{N}(0, \sigma^2)$$

Therefore, the ciphertext vector b is computed as follows:

$$b = A \cdot s + e_{\text{gaussian}}\, modq$$

For the second step, the Learning With Errors (LWE) problem, which is based on mixed Gaussian uniform noise, has been implemented. In this enhanced version of the problem, the error e_{mixed} is generated by combining Gaussian noise. As before matrix $A \in \mathbb{Z}_q^{m \times n}$ is randomly generated, Gaussian noise e_{gaussian} is sampled as follows:

$$e_{\text{gaussian}} \sim \mathcal{N}(0, \sigma^2)$$

Based on previous output, the discrete uniform noise e_{uniform} is sampled over the interval $[-a, a]$:

$$e_{\text{uniform}} \sim \text{Uniform}(-a, a)$$

Therefore, the combined error vector is identified as follows:

$$e_{\text{mixed}} = \left(e_{\text{gaussian}} + e_{\text{uniform}}\right) modq$$

The ciphertext vector b_{mixed} is computed simultaneously as follows:

$$b_{\text{mixed}} = A \cdot s + e_{\text{mixed}}\, modq$$

A simulation based on the equations and metrics for both the traditional and enhanced Learning With Errors (LWE) problems has been conducted, and the results are presented in the output cell of the code.

***Fig.4**. Performance Comparison output*

```
=== Traditional LWE (Gaussian Noise) ===
Matrix A (First 5 rows):
[[ 74  83  55   1  59  29  71  76  24  78  47  55  80  38  83  66  13  28
   41  32  23   0  70  94  52  96  16  32  54   4  80  70  91  51  24  33
   34  61  45  55  62  58  80  19  39  23  96  35  47  83]
 [  6  89  19  74  81  49  86  34  60  33  10  17  10  64  43  94  42  46
   60  30  22  24  53  53  92 100  80  41  76  68  74   7  87  80  44  35
   70  21  22  18  29  55  77  48  74  52  34  44  83  56]
 [  8  83   7  21  21  29  41  16  34  61  65   7  57 100  27  35  53  17
   24  33  97  28  53   1  37  39   0  30  96  80  82  46  21   4   3   4
    2  27  30  73  61  19  46  12  74  30  69  60  68  17]
 [ 24  43  36  25  65  23  94  59  73  83   6  42  37  78  49  50  62  94
   44  71  29  24  18  24  51  99  94  75   6  85  56  46  28  59  89  38
   47  98  75  22  99  89  62  26  38  34  24  90  71  30]
 [ 57  18  73  75  47  45  79  49  21  81 100  13  62  69  89  88   9  84
   17  67   0  85   8  96  38  33  75  42  74  11  17  63  30  46   3  36
   83  36  43  32  45  36  22  83  79  40  12  29  69   7]]
Vector b (First 5 elements):
[85  1 77 11 47]
Time Taken: 0.000285 seconds

=== Enhanced LWE (Gaussian + Uniform Noise) ===
Matrix A (First 5 rows):
[[ 49 100  27  96  91  55  93  65  94  62  76   9  91  88  61  12  41  27
   18  11  23  53  33  22  21  36  64  87   9  17  58  50  86  41  91  41
   40  54  59  26  79  35  73  55  54  16  57   5  10  54]
 [ 29  58  28  35  37  97  18  50  24  81  94  26  35  63  66  61  11  53
   58  95  61  71  12   4  88  54  84  75  86  77  80   9  45  21  36  61
   33  31  53  11  63   2  22  77  33   2  58  52  89  63]
 [ 57  68  84  68  52  79  61  18  13  61  10  77 100  58  87  58  67  78
   28  65  61  36  68  87  17  59  63  44  15  18  46  14   6  56  90  22
   21  29  30   3  58  10  82  63   6  50  97  99  24  50]
 [ 55  85  94  36  16  75  40  92  35   7  14  26  41  44  86  96  55  95
   89  32  69  15  24  44  95  52  74  71  54  77  11  19  40  81  46  68
   32  79  93  89  12  86  96  31  20  40  34  56   0  31]
 [ 77  25  53  30  49  58  38  76  47  35  31  97  39  96  56  64   3  70
   19  31  68  79   0  80  71  51  54  44   9  65  33  29  83  53  31  23
   33  33  81  68  94  62  38  82  72  35  42  97  56  28]]
Vector b (First 5 elements):
[28  9 52 63 82]
Time Taken: 0.000149 seconds

Performance Comparison:
Traditional LWE Time: 0.000285 seconds
Mixed LWE Time: 0.000149 seconds
Performance Difference: -0.000135 seconds
```

We can adjust the parameters and metrics and conduct multiple experiments to reduce noise and randomness, ultimately obtaining a mean performance comparison. The proposed simulation presents partial views of the matrix and vector generated by each method (Matrix A and Vector b). It includes a comparison of the computations for traditional Learning With Errors (LWE) and mixed error LWE, as well as a comparison of each model, highlighting the additional computational resources required for mixed LWE. Both the enhanced LWE problem with a mixed error distribution and the conventional LWE problem can be properly simulated by the provided code model. The two methods are compared in the results, highlighting any compromises between increased security and computing expense. This framework is a useful tool for examining post-quantum cryptography techniques since it can be effectively modified for larger datasets or further experimentation.

4. EXPERIMENTAL RESULTS

The experimental simulations presented are based on proposed models and were conducted using Python and its libraries. The objective was to compare the traditional Learning with Errors (LWE) problem against an enhanced version that incorporates a mixed error model. The implementation analyzed key performance metrics, including encryption and decryption times, resistance to attack

simulations, and overall efficiency. In the traditional LWE framework, the results were obtained using randomly generated parameters with dimensions m = 60 and b = 50, representing the public key. The ciphertext b was computed as b = a, where s is the secret vector and q = 101 is the modulus. The error vector e was sampled from a Gaussian distribution with a specified standard deviation, introducing predictable noise. In contrast, the enhanced version proposed a mixed LWE model that incorporates both Gaussian and uniform noise. In this case, the ciphertext vector and generated dimensions are identical to that in the traditional method. However, the error vector e_mixed is generated by combining samples from Gaussian noise and a uniform distribution over a specified interval. This mixed distribution introduces greater unpredictability.

4.1 PERFORMANCE COMPARISON

Metric	Traditional LWE (Gaussian Noise)	Enhanced LWE (Mixed Noise)
Encryption Time	0.000285 seconds	0.000149 seconds
Decryption Time	~0.000285 seconds (Assumed similar)	~0.000149 seconds (Assumed similar)
Error Distribution	Gaussian	Gaussian + Uniform
Security	Moderate	High

As shown in the comparison table, the enhanced LWE demonstrates a slight performance gain, contrary to the expectation of overhead, with the encryption time reduced approximately around 52.63% compared to the traditional LWE implementation. Because of the additional complexity involved in merging Gaussian and uniform noise, the mixed error distribution provides much higher security even with the improved efficiency. This increased complexity makes the LWE problem more resistant to both classical and quantum attacks. Attackers, especially those using quantum algorithms that take advantage of organized noise patterns, will find it more challenging to overcome the unpredictable nature of the mixed error distribution.

5. DISCUSSION

The results from the experiment showcase key insights into the excellence of the enhanced model, the viability of using mixed error distribution, and simultaneously provide ideas on how we can enhance the security of the Learning With Errors (LWE) problem by introducing interdisciplinary mathematical approaches. The enhanced LWE technique, which combines uniform and Gaussian noise, showed a significant increase in security, especially against attacks that take advantage of error regularities. While there will be a greater computational burden as a result, this trade-off is acceptable for applications that need higher post-quantum security.

5.1 LIMITATIONS AND FUTURE WORK

The results indicate that while the combination of mixed Gaussian and uniform noise distributions provides significant security enhancements, it also introduces increased computational overhead. To address this limitation, we propose that further research should explore alternative combinations of noise distributions or more complex models, incorporating quantum-safe distribution protocols. These protocols could enhance unpredictability without imposing substantial computational costs. Additionally, by integrating interdisciplinary approaches from mathematics, particularly number theory, we can propose mathematically defined hard problems. These problems would be defined in

such a way that they would be impossible or prohibitively expensive to solve with future quantum computers equipped with high qubit counts, which could potentially break RSA and current secure cryptographic protocols in a matter of minutes. Therefore, future work could involve more rigorous testing against quantum-specific attack models, including Grover's and Shor's algorithms, to evaluate how well the enhanced Learning With Errors (LWE) problem or other proposed models hold up in a quantum computing environment. Additionally, future research can leverage advancements in artificial intelligence (AI). AI is one of the most critical aspects of future cyber environments, and there have already been experiments aimed at creating AI-based firewall systems. More narrowly, researchers are implementing AI in cryptography by developing neurocryptographic hybrid systems for improved cryptanalysis and automated encryption protocols (Baklaga 2024b, 39–49). With this approach, future studies could explore interdisciplinary methods that integrate post-quantum cryptography and neural network-based cryptographic systems. In conclusion, the improved LWE problem with mixed noise presents a viable path toward creating quantum-resistant cryptographic systems that are more secure. The slight computational overhead is offset by the substantial gains in security, making this method a viable candidate for applications requiring strong post-quantum defenses.

ETHICAL STATEMENT

This study does not contain any studies with human or animal subjects performed by any of the authors.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to this work.

REFERENCES

1. Hasan, Khondokar Fida, Mir Ali Rezazadeh Baee, Leonie Simpson, Chadni Islam, Ziaur Rahman, Warren Armstrong, Praveen Gauravaram, and Matthew McKague. 2024. "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies." IEEE Access.
2. Baklaga, Luka. 2024. "Quantum-Resistant Lattice-Based Cryptography: New Conjectures on the Learning With Errors Problem." Scientific and Practical Cyber Security Journal 81: 50–56.
3. Baklaga, Luka. 2024. "Neuro-Cryptographic Hybrid Systems: Unleashing the Power of Neural Networks for Cryptanalysis and Encryption." Scientific and Practical Cyber Security Journal 81: 39 – 49.
4. Schneier, Bruce. 2022. "NIST's Post-Quantum Cryptography Standards Competition." IEEE Security & Privacy 20, no. 5: 107–108.
5. Bavdekar, Ritik, Eashan Jayant Chopde, Ankit Agrawal, and Kamlesh Tiwari. 2023. "Post Quantum Cryptography: A Review of Techniques, Challenges, and Standardizations." In 2023 International Conference on Information Networking (ICOIN).
6. Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen, eds. 2009. *Post-Quantum Cryptography*. Berlin: Springer.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 74 – 83 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CHALLENGES AND OPPORTUNITIES OF AI-DRIVEN CYBERSECURITY FOR SMALL AND MEDIUM ENTERPRISES (SMES) TOWARDS POVERTY REDUCTION IN NIGERIA

Ayepeku Olukayode FELIX[1], Olofinlade Samuel OLUWAPELUMI[2]

[1]Department of Mathematical and Computing Science, Thomas Adewumi University Oko-Irese, Kwara State, Nigeria
[2]University of Ilorin, Department of Accounting and Finance, Ilorin, Kwara State, Nigeria

ABSTRACT: Nigerian Small and Medium Enterprises (SMEs) face significant challenges in protecting their digital assets due to the increasing proliferation of cyber threats which tends to affect their goals of intermediary in employment generation towards reducing poverty in the society. This article examines the role of artificial intelligence (AI) in reducing risks and opening new opportunities for the SMEs in safeguarding their assets towards job creation which is an agent of fighting poverty to actualise SDGs. Limited resources, financial constraints, and a lack of awareness about cybersecurity risks contribute to the challenges faced by SMEs. However, the integration of AI-driven cybersecurity solutions offers significant opportunities. AI enhances threat detection capabilities, providing real-time analysis and rapid response mechanisms. Automation of routine tasks reduces the burden on limited resources and ensures a more proactive approach to cyber defence. AI solutions tailored for SMEs offer cost-effective options to bolster their cybersecurity posture. The article delves into case studies of successful implementation of AI-driven cybersecurity measures and explores government initiatives and support programs aimed at assisting SMEs in adopting these technologies. Collaborative approaches, information sharing, and employee training are crucial best practices for SMEs in navigating the evolving threat landscape. The article concludes by discussing emerging trends in AI-driven cybersecurity for SMEs and emphasizing their pivotal role in fostering sustainable business growth and resilience against cyber threats in Nigeria.

KEYWORDS: AI, AI-Driven, Cybersecurity, Enterprises, SMEs, Small, Medium, Poverty reduction, JEL Classification: G 21, G33.

1. INTRODUCTION

Cybersecurity faces an ever-evolving landscape of threats, including sophisticated malware, ransomware attacks, and vulnerabilities in software and networks. Artificial Intelligence (AI) has emerged as a powerful tool in enhancing cybersecurity capabilities, offering advanced features for threat detection, response, and mitigation. However, Nigeria's Small and Medium Enterprises (SMEs) are not left out of the threats as the SMEs tailored objective of provision of small assistance for economic growth are grappling with a mounting wave of cyber threats that pose significant risks to their operations and overall cybersecurity resilience towards the attainment of their objectives. This comprehensive exploration delves into the evolving threat landscape, highlighting the specific challenges faced by SMEs in Nigeria. Small and Medium-sized Enterprises (SMEs) are increasingly becoming targets for cyber-attacks due to several factors. These attacks can have severe consequences for these businesses, ranging from financial losses to reputational damage and the attainment of SDGs goal tend not to be actualised, and high poverty rates persist in many target states in the countries. As a result, in 2015, ending poverty (measured by people living on less than $1.20 per day) became the top precedence of the United Nations member states' global Sustainable Development Goals (SDGs) 2030 agenda. The global objectives of the United Nations aimed to end poverty and shield the planet by 2030. Sadly, the COVID-19 global pandemic has left substantial evidence of inevitable future poverty growth with the threat of financial and technological challenges. These cyber-attacks, often characterized by advanced persistent threats (APTs), exploit vulnerabilities in SMEs' networks and systems. (Ibitamuno 2023). The World Economic Forum's Global Risks Report points to the growing concern of supply chain vulnerabilities for Nigerian businesses. SMEs, often interconnected within extensive supply chains, are increasingly susceptible to attacks targeting third-party suppliers, which can result in significant disruptions. (“World Economic Forum: Global Risks Report 2019” 2019). A recent survey in Nigeria highlights a

concerning lack of cybersecurity awareness among employees of SMEs. This knowledge gap contributes to the success of various cyber-attacks, including those leveraging social engineering and insider threats, emphasizing the need for targeted awareness programs. ("Cybersecurity, Privacy, and Data Protection: State of the Art in Iran, Nigeria, Portugal, and the USA." 2023).

AI technologies, such as machine learning (ML) and deep learning, enable cybersecurity systems to analyze vast amounts of data rapidly. By learning from historical patterns and anomalies, AI-driven systems can identify potential threats that may go unnoticed by traditional signature-based methods. Real-time threat detection and prevention are critical components in safeguarding systems and networks from evolving cyber threats. (Maurya 2023). AI-driven cybersecurity solutions excel in behavioral analysis, allowing them to understand normal user behavior and identify deviations that may indicate a security threat. This proactive approach helps in early detection of anomalous activities, reducing the time it takes to respond to potential breaches. (Deepshikha Aggarwal, Deepti Sharma, Archana B. Saxena**,** 2023). AI-powered automation streamlines the response to security incidents. It enables rapid decision-making and executes predefined responses to mitigate threats. This is particularly crucial in dealing with fast-spreading malware and minimizing the impact of cyberattacks. (Tonhauser and Ristvej 2023). AI-driven cybersecurity solutions have the capacity to adapt and evolve based on new threat intelligence. Machine learning algorithms continuously learn from new data, allowing them to improve their accuracy over time. This self-learning capability enhances the resilience of cybersecurity systems against emerging threats. (Gheibi, Weyns, and Quin 2020)

2. CHALLENGES FOR SMES IN NIGERIA

The growing inclination of poverty is an exceptionally long-standing problem particularly in the North eastern regions of Nigeria which is prone to different security breach, many people as many people live below the poverty line and this poverty level continues to increase. Food and nutritional insufficiencies have reached a monumental proportion with malnourishment causes underweight in infants is a bane to attainment of SMEs goals. The multiplier effect of this bane on Small and Medium-sized Enterprises (SMEs) in Nigeria is part of numerous faces of challenges, and one significant hurdle is the limited availability of resources, particularly financial constraints. This challenge prevents SMEs from investing in advanced cybersecurity measures.

SMEs in Nigeria often operate within tight budgets, allocating resources to various aspects of their business operations. Limited financial resources present a significant challenge when it comes to addressing the complex and evolving landscape of cybersecurity threats. It is often said that people in rural areas have ideas but no financial inclusion is essential to drive the micro and macroeconomics factors towards growth and development which is part of the objectives of SMEs. Investing the little available funds in advanced cybersecurity measures requires a substantial financial commitment which the SMEs does not have in excess. SMEs, constrained by paucity of fund and essential financial resources referencing budgetary limitations, may find it challenging to allocate sufficient funds to implement robust cybersecurity infrastructure and technologies. (Anuj Thapliyal, 2022). A cybersecurity system that is out of date due to a lack of funding may expose SMEs to sophisticated cyberattacks. Sensitive consumer and corporate data may be in danger due to this low investment's insufficient defense against cyberattacks. SMEs that do not invest enough in cybersecurity solutions are more vulnerable to ransomware, phishing, and data breaches, among other cyberthreats. There might be serious interruptions to corporate operations if there are insufficient protection systems. (Kariuki, Ofusori, and Subramaniam, 2023).

Inadequate cybersecurity measures expose SMEs to potential reputational damage and regulatory penalties. Data breaches and cyber incidents can erode customer trust, impacting the company's reputation and potentially leading to legal consequences. According to a survey conducted by Ugwuja, V. C., Ekunwe, P. A., & Henri-Ukoha, A. (2020), a significant percentage of SMEs in Nigeria lack a comprehensive understanding of cybersecurity risks. SMEs often face challenges due to limited investment in training their employees on cybersecurity best practices. A study by Benz

and Chatterjee (2020) highlighted that only 40% of SMEs provide regular cybersecurity training to their staff. SMEs may struggle with understanding and complying with cybersecurity regulations. Marotta and Madnick 2020 emphasized the need for simplified guidelines and increased support for SMEs to navigate and adhere to cybersecurity regulations. Failure can lead to increased risk of cyber-attacks, data breaches, loss of sensitive information, financial losses, identity theft and fraud, reputation damage, the spread of malicious software, and weakened national security, to mention but a few. Insufficient awareness of available AI-driven solutions in cybersecurity is a significant challenge, impacting the ability of organizations to defend against evolving cyber threats. AI is instrumental in enhancing cybersecurity detection of sophisticated threats, real-time incident response, and automation of routine tasks. Moreover, lack of education and training also contributes to a gap in understanding among employees and decision-makers. Misconceptions and overreliance on AI can lead to unrealistic expectations and potential oversights in cybersecurity strategy. Global variations in awareness levels vary across regions, with more technologically advanced regions generally being more informed. The awareness of AI-driven cybersecurity solutions varies across different industries, regions, and organizational sizes. Large enterprises and tech-savvy industries generally exhibit higher levels of awareness, as they are more likely to invest in cutting-edge cybersecurity measures.

Cybersecurity professionals are well-informed about the capabilities and potential of AI-driven solutions, and increased media coverage and industry reports have contributed to greater awareness. However, SMEs and non-technical industries often lag in awareness due to limited resources, budget constraints, and a lack of dedicated IT personnel. According to (Bada & Nurse, 2019) SMEs in Nigeria often lack awareness and education about cybersecurity, leading to a lack of understanding of potential risks and consequences of cyber threats. This lack of awareness can increase their vulnerability to social engineering attacks and other cyber threats. Regional disparities and regulatory influence also play a role in fostering awareness about AI-driven solutions. The future outlook for AI-driven cybersecurity is expected to see rising interest and investments due to the ongoing rise in cyber threats and the recognition of AI's potential. Education and training initiatives will contribute to increased awareness, and the integration of AI tools and solutions into mainstream operations will expose a broader audience to its capabilities and benefits. Many Nigerian SMEs face financial constraints, hindering their ability to invest in robust cybersecurity measures. This insufficient budget makes them more susceptible to cyber threats, affecting their overall security. (Joseph, Obikaonu, Ariolu, Nwolisa, & Aderohunmu, 2021). Many Nigerian SMEs lack the latest cybersecurity technologies due to outdated IT infrastructure and lack of technology adoption. This vulnerability leaves them vulnerable to cybercriminals, as they may not have the latest security patches or defenses against evolving threats. (Reference: Oluwaseyi, J. O., & Afolayan, A. M. (2020). "Challenges of IT Infrastructure in Nigerian SMEs." International Journal of Computer Applications, 182(18), 43-48.) Nigerian SMEs face challenges in recruiting and retaining skilled cybersecurity professionals due to competition with larger enterprises. This shortage leaves them without the expertise to develop and maintain effective cybersecurity strategies, increasing their vulnerability to attacks. (Kassar, 2023). Nigerian SMEs face regulatory compliance challenges in cybersecurity, potentially leading to legal consequences and reputational damage. Clear and accessible guidelines are crucial to address these challenges and ensure compliance for SMEs. (Ukwuoma, Williams, & Choji, 2022)

3. OPPORTUNITIES PRESENTED BY AI-DRIVEN CYBERSECURITY

This paper discusses the potential of AI-driven cybersecurity for Small and Medium Enterprises (SMEs) in Nigeria towards poverty reduction. AI-driven cybersecurity solutions can automate threat detection and response, reducing response times and enhancing the speed of response.

Predictive analytics can also be used for proactive defence, allowing SMEs to implement pre-emptive measures before they escalate into major security incidents that can have negative impact of food security thereby enhancing poverty alleviation. AI-driven cybersecurity solutions can be customized to suit the specific needs and scale of SMEs, offering flexibility and scalability. Behavioural biometrics, facial recognition, and anomaly detection algorithms can enhance user authentication and access control, reducing the risk of unauthorized access. (Gaggero, Girdinio, & Marchese, 2021)

AI-driven cybersecurity solutions can also be cost-effective through resource optimization. Automated threat detection and response mechanisms reduce the need for extensive human intervention, allowing SMEs to allocate resources efficiently. This cost-effectiveness enhances the affordability of advanced cybersecurity measures and makes it an attractive option for SMEs in Nigeria. Overall, AI-driven cybersecurity offers a promising solution for SMEs in the digital age. (Bhardwaj & Kaushik, 2022)

Artificial Intelligence (AI) is revolutionizing cybersecurity by enhancing threat detection capabilities through advanced analytics, automation, and machine learning. AI algorithms can detect anomalies by establishing a baseline of normal behaviour, while behavioural analysis allows AI to analyse user and entity behaviour to identify deviations from typical patterns. Machine learning models enable AI to analyse vast amounts of data, improving accuracy in identifying known and unknown threats. AI can integrate threat intelligence feeds and databases to stay updated on the latest known threats, reducing the time to detect and respond to emerging threats. (Alfayoumi, Eltazi, & Elgammal, 2023). Predictive analysis allows AI to predict potential threats based on historical data and ongoing trends, allowing organizations to proactively address emerging threats before they escalate. AI-driven automation can handle routine security tasks, freeing up human resources to focus on more complex threat analysis and response. Deep learning for image and speech recognition enhances detection capabilities in areas like video surveillance and voice command systems. Dynamic threat modelling allows AI to dynamically model evolving threats based on real-time data, providing a more accurate and adaptive threat detection system. (El- El-Sofany, 2022)

AI plays a crucial role in various aspects of cybersecurity, including threat detection, log analysis, incident triage, vulnerability assessment, and phishing detection which the SMEs can benefit from in attending to its pivotal goals. AI-powered tools process and correlate logs from multiple sources to identify anomalies and potential security events, while automated incident response platforms triage incidents, prioritize critical ones, and provide comprehensive reports on potential vulnerabilities. To make AI solutions scalable and affordable for Small and Medium Enterprises (SMEs), a strategic approach considering resource constraints, cost-effectiveness, and specific requirements is needed. Strategies include using cloud-based AI services and platforms, leveraging open source AI tools, choosing modular and customizable solutions, exploring pre-built AI solutions, prioritizing AI applications that align with core business objectives, adopting AI as a Service (AIaaS), incremental implementation, employee training and upskilling, low-code/no-code platforms, regular evaluation and optimization, and exploring government initiatives and grants.

Artificial Intelligence (AI) is revolutionizing cybersecurity for Nigerian Small and Medium Enterprises (SMEs) by enabling real-time analysis of patterns and anomalies. AI-powered systems monitor network activities, user behaviours, and system logs, identifying potential threats as they emerge. It excels in pattern recognition, allowing it to distinguish normal behaviour from anomalies. AI can also help mitigate zero-day threats by recognizing patterns associated with previously unseen threats. AI-driven solutions conduct behavioural analysis for insider threats, raising alerts in case of suspicious behaviour. These solutions are scalable and affordable, contributing to regulatory compliance requirements in industries with stringent data protection and privacy regulations. (Rizvi, 2023). The integration of Artificial Intelligence (AI) in automated incident response systems offers Nigerian SMEs a significant opportunity on innovative financial

programmes and reforms that can support entrepreneur financing poverty reduction mechanism. AI-driven systems enable real-time threat mitigation, allowing for immediate identification and mitigation of cyber threats. This is particularly beneficial for SMEs in Nigeria, where speed of response minimizes the impact of security incidents. AI algorithms analyse incoming threat data in real-time, aligning incident response strategies with the latest threat landscape. This reduces response time, reducing damage and disruptions. AI systems also learn from past incidents, adapting response strategies over time. Continuous monitoring and analysis of network activities further enhance the effectiveness of AI-powered systems. (Chahal, 2023)

The digital age presents significant opportunities for Small and Medium Enterprises (SMEs) in Nigeria, particularly when leveraging AI-driven cybersecurity solutions. Key opportunities include proactive threat detection and prevention, cost-effective security measures, tailored solutions, enhanced incident response capabilities, government support and incentives, global competitiveness, cybersecurity skills development, data privacy and compliance, innovation and digital transformation, collaborative threat intelligence sharing, business resilience and continuity, customizable training programs, market differentiation, and ecosystem collaboration. Proactive threat detection and prevention enable SMEs to identify patterns indicative of potential attacks and take preventive measures, reducing the risk of data breaches. Cost-effective security measures reduce the need for extensive human intervention, allowing SMEs to enhance their cybersecurity posture without significant resource investments. Tailored solutions for SMEs address their unique needs and challenges, while automated incident response minimizes the impact of security breaches, reducing downtime and potential financial losses. Governments and regulatory bodies may offer support and incentives for SMEs adopting AI-driven cybersecurity measures, making advanced technologies more accessible. Implementing AI-driven cybersecurity can enhance global competitiveness, build trust with international partners and customers, and improve cybersecurity skills development among the workforce. AI can also aid SMEs in ensuring data privacy and compliance with regulatory requirements, building a reputation for secure and compliant operations.

AI-driven cybersecurity aligns with the broader trends of innovation and digital transformation, attracting customers who prioritize security in their partnerships. Collaborative threat intelligence sharing among SMEs and within industry networks benefits SMEs from shared insights, collective defence mechanisms, and a collaborative approach to combating cyber threats. Customizable training programs for SMEs enhance the overall security culture and help SMEs differentiate themselves in the market. Ecosystem collaboration within the cybersecurity ecosystem, including partnerships with service providers, strengthens SMEs' overall cybersecurity defences.

4. CASE STUDIES

AI-driven cybersecurity measures are increasingly being adopted by SMEs worldwide to improve their security posture for risk reduction. These solutions offer benefits such as real-time threat detection, endpoint protection, user and entity behavioural analytics (UEBA), automated incident response, cloud security, phishing detection, network traffic analysis, and security orchestration and automation response (SOAR). In Nigeria, AI-driven cybersecurity has shown potential positive impacts on SMEs business operations, including improved threat detection, endpoint protection, proactive insider threat detection, cloud security enhancement, phishing prevention, efficient network traffic analysis, and enhanced data privacy and compliance. However, the outcomes may vary depending on the specific context and implementation of AI-driven cybersecurity solutions. The e-commerce industry in Nigeria faces challenges and different risk such as business model risk, operational costs, and user disposable income. However, the market is rapidly growing, projected to reach $75 billion by 2025 and $120 billion by 2030. This growth is driven by factors such as the growing youthful population, increasing internet penetration in rural areas, rising disposable

incomes, and a growing middle class. The market's success depends on overcoming these challenges and leveraging Nigeria's FX reserve and economic growth through maintaining appropriate levels of investment, particularly in infrastructure This is crucial to attaining this aim of job opportunities, employment growth which should be made available for the youth through small and medium business towards self-reliant and be an employer of labour from their small-scale enterprises with their entrepreneur innovative efforts and lots more which the AI can safeguard

5. GOVERNMENT INITIATIVES AND SUPPORT

The Nigerian government has implemented several initiatives to support SMEs in enhancing their cybersecurity. These include the National Cybersecurity Policy and Strategy, which aims to create a secure cyberspace for individuals and businesses, and guidelines issued by the National Information Technology Development Agency (NITDA) on data protection. The government has also initiated capacity building programs to enhance SMEs' cybersecurity skills through training sessions, workshops, and seminars towards reducing the cyber security challenges and business systematic and unsystematic risk which is a bane to Nigeria business environment. Opportunities for AI-driven cybersecurity in SMEs include automation and threat detection, collaborative initiatives between SMEs and government agencies, and incentives for adoption. These can help mitigate the challenges posed by limited resources and promote the adoption of advanced protective measures. Additionally, the government can introduce tax breaks or grants to encourage SMEs to invest in AI-driven cybersecurity solutions, alleviating budget constraints and promoting the adoption of advanced protective measures. Government initiatives to promote cybersecurity in Small and Medium Enterprises (SMEs) are crucial for ensuring the resilience of the national cybersecurity landscape. These initiatives include cybersecurity awareness campaigns, training and capacity building programs, access to cybersecurity resources, incident response support, regulatory compliance assistance, financial support and grants, information sharing platforms, national cybersecurity standards for SMEs, public-private partnerships, cybersecurity insurance awareness, and international collaboration.

These initiatives aim to increase awareness among SMEs about cybersecurity threats and best practices, provide affordable access to cybersecurity tools and resources, assist SMEs in responding to and recovering from cyber incidents, and help them understand and comply with cybersecurity regulations. Financial support and grants are also offered to SMEs for investing in cybersecurity infrastructure, training, and technology. Information sharing platforms facilitate the exchange of cybersecurity threat intelligence among SMEs, while national cybersecurity standards are defined and disseminated. Public-private partnerships foster collaboration between government agencies, industry associations, and SMEs to discuss cybersecurity challenges and solutions. Cybersecurity insurance awareness encourages SMEs to consider it as part of their risk management strategy. International collaboration facilitates international cooperation on cybersecurity matters affecting SMEs.

AI-driven cybersecurity measures can be challenging for small and medium-sized enterprises (SMEs) due to resource constraints. Governments, industry bodies, and other organizations offer support programs to help SMEs adopt advanced cybersecurity technologies. These programs include government grants and subsidies, cybersecurity voucher programs, public-private partnerships, training and capacity building programs, technology adoption consultancy services, innovation and technology development funds, access to cybersecurity research and development resources, cybersecurity competitions and challenges, international collaboration programs, cybersecurity certification assistance, industry-specific support, and cybersecurity awareness campaigns. These programs provide financial assistance to offset costs associated with implementing AI solutions, enhance skills and knowledge, and provide access to global expertise and insights. SMEs should seek information about these programs from government cybersecurity

agencies, industry associations, and business development organizations, and collaborate with local technology hubs, innovation centers, and industry networks for valuable insights and opportunities for support.

6. FUTURE OUTLOOK

The future of AI-driven cybersecurity for Small and Medium Enterprises (SMEs) in Nigeria presents both challenges and opportunities. Rapid technological change is expected to accelerate, requiring SMEs to adapt quickly to new solutions. The increasing sophistication of cyber threats necessitates the investment in AI-driven solutions that can dynamically adapt to evolving threat landscapes and offer advanced threat detection capabilities. The rising demand for skilled cybersecurity professionals will likely increase, exacerbating the existing skills gap. SMEs may face challenges in recruiting and retaining qualified talent, emphasizing the need for training and upskilling programs. Integrating AI-driven cybersecurity solutions with legacy systems may be challenging, necessitating infrastructure upgrades and compatibility. Opportunities include advances in user-friendly AI solutions, government support and initiatives, collaborative cybersecurity ecosystems, and the rise of tailored AI solutions for SMEs. Governments may increase support and initiatives to help SMEs bolster their cybersecurity capabilities, such as grants, subsidies, and training programs. Collaborative efforts between SMEs, industry partners, and cybersecurity providers may strengthen the overall cybersecurity ecosystem. Tailored AI solutions for SMEs can be cost-effective, scalable, and address specific cybersecurity requirements. Strategic considerations for SMEs include investing in continuous training, embracing collaboration, planning for the agile adoption of emerging technologies, exploring government support programs, and conducting thorough assessments of their existing IT infrastructure to ensure compatibility with AI-driven cybersecurity solutions.

AI-driven cybersecurity for Small and Medium Enterprises (SMEs) is undergoing significant advancements, including AI-powered threat hunting, Zero Trust Security Architecture, Extended Detection and Response (XDR), Behavioral Biometrics, AI in Endpoint Detection and Response (EDR), Explainable AI (XAI), AI for Insider Threat Detection, AI-Enhanced Cloud Security, Adversarial Machine Learning Defense, AI-Driven Automation in Incident Response, AI-Powered Phishing Detection, AI Governance and Ethical AI, and Edge AI for IoT Security. These technologies will enhance threat detection and response, comply with evolving cybersecurity regulations, and make advanced cybersecurity solutions more accessible to SMEs. However, challenges such as adversarial AI attacks, ethical concerns, resource constraints, regulatory complexity, and overreliance on AI without human oversight will need to be addressed. A concerted effort from governments, industry stakeholders, and cybersecurity professionals is needed to ensure responsible and effective integration of AI in SME cybersecurity strategies.

The future of AI-driven cybersecurity in Nigerian SMEs is expected to see increased adoption rates due to growing awareness of cyber threats and the need for advanced security solutions. Advances in AI technology may lead to more affordable and accessible solutions tailored for SMEs, enabling a broader range of businesses to implement robust security measures. Regulatory authorities in Nigeria may place increased emphasis on cybersecurity measures, encouraging SMEs to adopt AI-driven solutions to meet compliance requirements and protect sensitive data. AI cybersecurity solutions may become more customizable to suit the specific needs and resource constraints of SMEs, making it easier for them to implement and manage these technologies effectively. With the growing reliance on cloud services, AI-driven cybersecurity solutions may integrate with cloud security measures, providing comprehensive protection for SMEs operating in cloud environments. Collaboration and partnerships with cybersecurity service providers and technology firms may be increased to access expertise and deploy AI-driven solutions effectively. The Nigerian government may implement initiatives to support SMEs in enhancing their cybersecurity posture, offering

incentives or guidance for the adoption of AI-driven solutions. AI-driven threat hunting may play a more prominent role in proactive threat hunting, while quantum computing threat preparedness may lead to more user-friendly interfaces.

CONCLUSION AND RECOMMENDATIONS

SMEs in Nigeria face several challenges in understanding cybersecurity risks, including limited awareness, a lack of dedicated cybersecurity personnel, resource constraints, and insufficient awareness of available AI solutions. Government initiatives and support programs can help SMEs enhance their cybersecurity measures, while collaboration and information sharing can foster a stronger cybersecurity ecosystem. Advancements in AI technologies offer scalable, adaptive, and cost-effective cybersecurity solutions, and innovations in cybersecurity awareness training empower SME employees to identify and respond to cyber threats. Embracing AI-driven cybersecurity is crucial for sustainable growth, protecting SMEs from financial losses, enhancing business reputation, and ensuring compliance with cybersecurity regulations. Tailored solutions for local challenges, supporting digital transformation, job creation and skill development, and enhancing global competitiveness are some of the benefits of AI-driven cybersecurity. The Nigerian Communications Commission reports that cybercrime costs Nigeria billions of dollars annually, making it crucial for SMEs to adopt AI-driven cybersecurity. Tailored solutions can address specific cyber threats, support digital transformation initiatives, and stimulate job creation and skill development. Furthermore, cybersecurity readiness enhances global competitiveness, allowing SMEs in Nigeria to compete more effectively on the global stage.

Adequate training for local security networks and agencies is crucial and can be effective in offering local intelligence gathering and thereby pass it over to the appropriate military or established intelligence unit where such information is vital and essential. Funding: No funding, grants, or other support were received. Conflict of interest: The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

Aggarwal, D., Sharma, D., & Saxena, A.B. 2023. 'Role of AI in Cyber Security through Anomaly Detection and Predictive Analysis.' *Journal of Informatics Education and Research.* Available at: https://doi.org/10.52783/jier.v3i2.314.

Alfayoumi, S., Eltazi, N., & Elgammal, A. 2023. 'AI-Driven Optimization Approach Based on Genetic Algorithm in Mass Customization Supplying and Manufacturing.' *International Journal of Advanced Computer Science and Applications* 14(11). Available at: https://doi.org/10.14569/ijacsa.

Bada, M., & Nurse, J.R. 2019. 'Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).' *Information & Computer Security* 27(3), pp. 393–410. Available at: https://doi.org/10.1108/ics-07-2018-0080.

Benz, M., & Chatterjee, D. 2020. 'Calculated Risk? A Cybersecurity Evaluation Tool for SMEs.' *Business Horizons* 63(4), pp. 531–40. Available at: https://doi.org/10.1016/j.bushor.2020.03.010.

Bitamuno, P.V. 2023. 'Legal Frameworks for Cybersecurity in Nigeria - Adapting The Fourth Industrial Revolution.' *Advances in Multidisciplinary and Scientific Research Journal*

Publication 2(1), pp. 97–104. Available at: https://doi.org/10.22624/aims/cseansmart2023p12

Bhardwaj, A., & Kaushik, K. 2022. 'Predictive Analytics-Based Cybersecurity Framework for Cloud Infrastructure.' *International Journal of Cloud Applications and Computing* 12(1), pp. 1–20. Available at: https://doi.org/10.4018/ijcac.297106.

Chahal, S. 2023. 'AI-Enhanced Cyber Incident Response and Recovery.' *International Journal of Science and Research (IJSR)* 12(3), pp. 1795–1801. Available at: https://doi.org/10.21275/sr231003163025.

Gaggero, G.B., Girdinio, P., & Marchese, M. 2021. 'Advancements and Research Trends in Microgrids Cybersecurity.' *Applied Sciences* 11(16), pp. 7363. Available at: https://doi.org/10.3390/app11167363.

Gheibi, O., Weyns, D., & Quin, F. 2020. 'Applying Machine Learning in Self-Adaptive Systems.' *ACM Transactions on Autonomous and Adaptive Systems* 15(3), pp. 1–37. Available at: https://doi.org/10.1145/3469440.

International Journal of Marketing, Communication and New Media. 2023. 'Cybersecurity, Privacy, and Data Protection: State of the Art in Iran, Nigeria, Portugal, and the USA.' February. Available at: https://doi.org/10.54663/2182-9306.2023.sn12.1-4.

Joseph, T., Obikaonu, P., Ariolu, C., Nwolisa, C., & Aderohunmu, A. 2021. 'SMEs Intervention Programmes in Nigeria: Evaluating Challenges Facing Implementation.' *Applied Journal of Economics, Management and Social Sciences* 2(1), pp. 16–25. Available at: https://doi.org/10.53790/ajmss.v2i1.10.

Kariuki, P., Ofusori, L.O., & Subramaniam, P.R. 2023. 'Cybersecurity Threats and Vulnerabilities Experienced by Small-Scale African Migrant Traders in Southern Africa.' *Security Journal* June. Available at: https://doi.org/10.1057/s41284-023-00378-1.

Kassar, G. 2023. 'Exploring Cybersecurity Awareness and Resilience of SMEs amid the Sudden Shift to Remote Work during the Coronavirus Pandemic: A Pilot Study.' *ARPHA Conference Abstracts* 6. Available at: https://doi.org/10.3897/aca.6.e107358.

Maurya, R. 2023. 'Analyzing the Role of AI in Cyber Security Threat Detection & Prevention.' *International Journal for Research in Applied Science and Engineering Technology* 11(11), pp. 514–19. Available at: https://doi.org/10.22214/ijraset.2023.56510.

Marotta, A., & Madnick, S.E. 2020. 'Analyzing the Interplay Between Regulatory Compliance and Cybersecurity.' *SSRN Electronic Journal.* Available at: https://doi.org/10.2139/ssrn.3542563.

Rizvi, M. 2023. 'Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention.' *International Journal of Advanced Engineering Research and Science* 10(5), pp. 055–060. Available at: https://doi.org/10.22161/ijaers.105.8.

Thapliyal, A. 2022. 'Importance of Cybersecurity in Financial Services Industry: An Analytical Perspective of Various Security Models.' *International Journal of Early Childhood Special Education* June. Available at: https://doi.org/10.48047/intjecse/v14i2.1074.

Tonhauser, M., & Ristvej, J. 2023. 'Cybersecurity Automation in Countering Cyberattacks.' *Transportation Research Procedia* 74, pp. 1360–65. Available at: https://doi.org/10.1016/j.trpro.2023.11.283.

Ugwuja, V.C., Ekunwe, P.A., & Henri-Ukoha, A. 2020. 'Cyber Risks in Electronic Banking: Exposures and Cybersecurity Preparedness of Women Agro-Entrepreneurs in South- South Region of Nigeria.' *Journal of Business Diversity* 20(3), September. Available at: https://doi.org/10.33423/jbd.v20i3.3087.

Ukwuoma, H.C., Williams, I.S., & Choji, I.D. 2022. 'Digital Economy and Cybersecurity in Nigeria.' *International Journal of Innovation in the Digital Economy* 13(1), pp. 1–11. Available at: https://doi.org/10.4018/ijide.292489.

World Economic Forum. 2019. 'Global Risks Report 2019.' *Computer Fraud & Security* 2019(2), pp. 4–4. Available at: https://doi.org/10.1016/s1361-3723(19)30016-8.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 84 – 91 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

NOVEL RANDOM ENCRYPTION METHODS BASED ON MUTATION STRATEGIES OF ARTIFICIAL INTELLIGENCE

Rangel-Lugo, Edgar [1] and Rangel-Ríos, Kevin Uriel [2]

[1]Tecnológico Nacional de México
[2]Instituto Tecnológico de Ciudad Altamirano

ABSTRACT: The theft of digital data problem is receiving growing attention. This situation, when occurs in several practical domains, it may produce an important loss in an organization's finances. In this paper, several aspects related to this subject are studied. We focus on cybersecurity strategies based on random encryption methods to suggest replacement of the static encryption schema by another dynamic alternatives. The encryption method is considered dynamic if they can obtain a different ciphertext as a result with the same plaintext input. Novel definitions of random methodologies based on mutation strategies with Artificial Intelligence (AI) for camouflaging the ciphertext are also introduced.

KEYWORDS*:* Random encryption methods, applications of AI, cybersecurity strategies.

1. INTRODUCTION

A cybersecurity strategy (Delman 2004; Kalsi et al. 2018; Mendoza 2008; Rangel et al. 2023) is considered inadequate if at least one of the methods is vulnerable to cybercriminal attacks. Most of these cases refer to fraudulent telephone calls or phishing, social networking platforms, bank systems, large markets or retail supply chains, electrical energy network business, fraudulent financial sector situations, and several cases of e-commerce in organizations (Reddaiah 2019; Sebas 2023; Barranco and Galindo 2022; Gómez et al. 2012; Javidi et al. 1997; Cover and Hart 1967; Barandela et al. 2003; Rangel 2022; Álvarez 2019). This situation has been observed that the theft of digital data (Rangel et al. 2023) may cause significant losses in the finances of organisations. Most attempts to address this problem can be grouped into several categories: One is to periodically replace cybersecurity strategies. The second parameter is related to the employment of dynamic encryption methods (Delman 2004; Rangel et al. 2023; Reddaiah 2019; Fulgueira et al. 2015; Luciano and Prichett 1987; Linfei and Daomu 2005). Following the common practice, it can be observed that several alternatives (Delman 2004; Mendoza 2008; Rangel et al. 2023; Barranco and Galindo 2022; Gómez et al. 2012; Javidi et al. 1997; Álvarez 2019; Fulgueira et al. 2015; Luciano and Prichett 1987; Linfei and Daomu 2005; Pisarchik and Zanin 2008; Rajan and Saumitr 2006; Rueda et al. 2005; William 1999) for handling the theft of digital data problems have been employed. However, in this study, only two classes of situations were studied. First, the comparison of three random variants (Rangel et al. 2023) as dynamic encryption proposals because these methods have been rarely studied in the literature. Second, two modifications of the random methods (named here as *reduced random Caesar* and *reduced random mutation*) were implemented for downsizing to the ciphertext and it can increase the execution time of the encryption process. Here, both goals are considered dynamic alternatives to random performance.

As pointed out by some authors, random encryption methodologies, such as *random Caesar I* and *random Caesar II* (Rangel et al. 2023), offer a good alternative to increasing noisy and redundant information in ciphertext outputs. However, these methods can obtain random values for the ciphertext that are selected out of the range of the ASCII table. Consequently, in environments where the theft of digital data has occurred, other measures have been proposed. The ciphertexts based on the *pseudo-hexadecimal* format (Rangel et al. 2023) and the use of *nearest neighbor* (*1-NN)* supervised method (Cover and Hart 1967) with noise injection over hexadecimal encoding are good indicators of dynamic

encryption method performance in these domains. However, the obtained ciphertext outputs may be too large sequences. Therefore, these strategies were not employed in this study because our main proposal is concerned with downsizing and camouflaging the ciphertext.

The evaluation of these random encryption methods in previous research (Rangel et al. 2023) with five-fold cross-validation was experimented. In this work, the performance of those methods was expressed in terms of the global average or accuracy (Barandela et al. 2003). Hence, this paper presents preliminary results of a more extensive research, which it has been conducting to explore some cases related to the theft of digital data. It has studied in situations that were caused because at least one of the inadequate encryption method have been employed. Initially, the experiments were focused on replacing of the random encryption schemes for recommending the reduction of these obtained ciphertext with novel proposals (here named as *reduced random Caesar* and *reduced random mutation*). Of course, without to put in risk the data security of the organizations. Besides, several of the ciphertext exemplars obtained by those reduced and random encryption methods are here shown. These approaches were evaluated over five samples when a novel modification of cross-validation have been employed.

Finally, we propose the reduction of ciphertext output based on *random Caesar* methodology because is good indicators of the dynamical encryption performance. Hence, two modifications for downsizing of this encryption method is here recommended. Of course, this situation should not put in risk the digital data security in the organizations. Hence, two modifications of *random Caesar II* version (named here as: *reduced random Caesar* and *reduced random mutation*) for downsizing and camouflaging to the ciphertext are good indicators because can decrease the times of the encryption process without put in risk the data security.

2. RELATED THEORETICAL AND EXPERIMENTAL METHODS

Replacing the cybersecurity schemes, this situation does not guarantee the data security of the organisations, if the replacement consists on the employment of static encryption algorithms (Mendoza 2008; Barranco and Galindo 2022; Gómez et al. 2012; Rodríguez 2020; Telerik Progress Software Corporation 2022). In these cases is recommended using a dynamical encryption methods which they are able to obtain distinct ciphertext as results with the same plaintext input. This paper describes two groups of these selected encryption measures as alternative for handling to the theft of digital data problem.

First adopted strategy consists in the employment of random methods as dynamic data encryption performance because these schemes offer a good alternative for increasing noisy of the ciphertext outputs. In particular, the random Caesar I and *random Caesar II* versions were here employed, which are based on traditional *Caesar* (Barranco and Galindo 2022; Gómez et al. 2012; Rangel et al. 2023) algorithm, but they differ because *random Caesar* variants are dynamical encryption methods (Rangel et al. 2023) with AI based on random strategies such as genetic algorithms. The ciphertext based on traditional *Caesar* (by *shifting* variant) works with only one static *K* value, which can be defined as: $C_i = S_i + K \bmod 26$ (Barranco and Galindo 2022; Gómez et al. 2012). In case of the by *substitution* Caesar implementation, it can be computed as: $C_i = Z_i \bmod 26$. Where: $Z_i = D_t$, only if the S_i (plaintext) is equal than A_t, otherwise $Z_i = S_i$ is assigned because A_t vector corresponds to the original alphabet with 26 characters and D_t is the alphabet after of the shifting operation, which can be obtained as follows: $D_t = A_{(t+K)}$, if the (t+K) value is greater than *mod 26* then starts counting from the beginning again. However, the *random Caesar* methods the shift value (named here as K_i) can be selected a distinct for each character of the S_i plaintext because they are obtained randomly (with replacement). The *random Caesar* (Rangel et al. 2023) encryption method consists in two phases. First, the partial ciphertext is computed as $C_i = S_i + K_i \bmod N$. Second, corresponds to the package calculation, which can be defined as follows: $FinalPackage = C_i + K_i + OrdChr(C_i)$. Where, the K parameter is the shifting of the traditional *Caesar* (with k=3 value) and K_i vector are the selected random values which represents the shifts of the S_i plaintext. The partial encryption of the C_i vector is obtained with the *sum* operation while

that in *FinalPackage*, the + operator corresponds to the *concatenation* function, while the *OrdChr* procedure must put an integer (ordinal) value in the final of the ciphered sequence in case of the *random Caesar I* version. However, for the *random Caesar II* variants, should put the same character of C_i in final of the package (Rangel et al. 2023). Finally, the *mod N* value (Barranco and Galindo 2022; Gómez et al. 2012; Rangel et al. 2023), is the size of the encryption alphabet, where should be used the N=26 value for both traditional *Caesar* implementations here presented, and it must be employed the N=95 with the ASCII range values between 32 and 126 for *random Caesar I* version, and it should be assigned the N=120 with range of ASCII values between 30 and 150 for *random Caesar II* (Rangel et al. 2023). A second encryption strategy consists in the camouflaging and reduction of the obtained ciphertext by *random Caesar* methodologies. Nevertheless, because those ciphertexts are three-times bigger than plaintext, two random dinamic encryption methods were here proposed. Hence, in this research two modifications of the *random Caesar II* version have been employed for camouflaging and downsizing at least ⅓ of the ciphertext. These proposals are here named as *reduced random Caesar* and *reduced random mutation*. Both variants consist in two phases, following the same way that *random Caesar II*, but differs in the second phase. First, the procedure corresponds to the partial encryption process which can be computed with the *sum* of ordinals as follows: $C_i = S_i + K_i \ mod\ 120$. Second, the phase of the reduced random methods is the same package calculation of *random Caesar II*, but the last noised character is deleted for each sequence of C_i. Therefore, the encryption package of the *reduced random Caesar* can be obtained as: $FinalPackage = C_i + ((char)(K_i))$. We can observe that this package only the partial ciphertext and random K_i values are included , but K_i is camouflaged as ASCII character. Hence, for each K_i value should be in the range of shifting between 0 and 105 for does not exceed the 255 ASCII value. However, the second phase of the *reduced random mutation* alternative, differs because it is applied a *mutation operation* for swapping the K_i by C_i values as follows: $FinalPackage = (C_1 + ((char)(K_1))) + (((char)(K_2)) + C_2) + ... + (C_{i-1} + ((char)(K_{i-1}))) + (((char)(K_i)) + C_i)$. This situation can help to camouflage the information of the final package and avoids putting in risk the data security. On other hand, the employment of random methodologies, for the encryption of information has shown to obtain dynamical ciphertext results, which is good for the data security. However, this situation can produce too many errors when some sequence of characters is out of range to the ASCII table (Rangel et al. 2023) because the random K_i vector is not delimited. Hence, the employment of *reduced random* and *mutation* schemes can help to decrease errors of the encryption methods because they use alphabets with mod 120 (Rangel et al. 2023) and the range of K_i values are delimited between 0 and 105, which can help us avoid the ASCII values selection when are out of range (unless the plaintext contains non-ASCII characters), reason for which is here proposed as a novel dynamic encryption strategy too.

Regarding the evaluation of results, in this research, for internally biasing the discrimination procedure is proposed the cross-validation method (Barandela et al. 2003; Rangel et al. 2023). This information can help us recommend the employment of some dynamic strategies of the reduced and random encryption methods, in the organisations.

3. RESULTS AND DISCUSSION

All the experiments were carried out over five random samples of ciphertext where the execution of times with estimated error were included for each encryption method, separately (e.g., if plaintext is not equal than decryption ciphertext then, it is computed as error). The random ciphertext in samples were transformed with maximum size of 255 elements for each encryption sequence of the five-fold with a modified of cross-validation method, which has been employed to facilitate comparison with other published results (Barranco and Galindo 2022; Delman 2004; Gómez et al. 2012; Rangel et al. 2023). First, two traditional *Caesar* implementation versions by *shifting* and *substitution* variants (Barranco and Galindo 2022; Gómez et al. 2012) over five samples and K=4 values were employed. Second, three variants of *random Caesar* encryption methods (version I, version II *mod 95* and version II *mod 120*) were applied over the same five samples with only five repetitions, separately. Moreover, the novel *reduced random Caesar* and *reduced random mutation* proposals were also employed separately in an

iterative manner with the same five samples and five repetitions of cross-validation. In experiments, the global average has been computed with the modified cross-validation for each different encryption method, separately. Regarding the application of the novel cross-validation method, just one variant to the procedure has been carried out, which is described as follows. For each encryption method: (1) First, the encryption process over five samples has been employed with size of 20%. (2) One ciphered sample was sequentially extracted without replacement and the decryption process is applied over four samples that correspond the 80% of encryption data. (3) It is repeated five times the second step.

After processing all the samples for each encryption method, the average results were computed which are shown in *Table 1*. The columns A and B contain the results obtained with the employment of the global average and the standard deviation, respectively (the times of encryption and decryption was measured in milliseconds). The best balanced results are always obtained when the reduced random alternatives were employed. In all samples, this measure alone produces a considerable improvement in the trust for each encryption method performance. Thus, the reduced random schemes show themselves is a good resource to conduct the experimentation procedures, although other factors must be still analyzed.

On the other hand, benefits of *random Caesar* methods are well-known for increasing the data security in organisations (Rangel et al. 2023). In *Table 1*, this effect was corroborated for the computed global average. The same can be stated about the results obtained when processing the *reduced random* and *mutation* alternatives because too short ciphertext is produced. Therefore, the execution of times are smaller than the other proposals here presented. This situation can achieve that the cybercriminals do not delay too much in the decryption process, but in this case, they should have known each random K_i value, which has been camouflaged previously. These tasks of data discovering might be very difficult.

Repeated application of *random* encryption methods can help us obtain dynamical and better results in comparison with the traditional *Caesar* algorithm. In this work, the iterative procedure of the experiments was stopped when five repetitions of ciphertext were produced with reduced and random strategies. In case of the traditional *Caesar* algorithm were executed some experiments with K=4 value, where has been observed that traditional *Caesar* algorithm, suffers not only from the data security problem, but also the times of ciphertext are too large in comparison with reduced *random* and *mutation* alternatives (see *Table 1*).

The methodologies based on *random Caesar* have shown to be faster than the other traditional *Caesar* proposals here evaluated. However, these schemes can produce vulnerability to the data security in the organisations and might be very good for the cybercriminal decryption strategies. However, the downsized ciphertext with *reduced random* methods, they can be considered very good recommendation. This schema does not put in risk data security of the information because in the ciphertext have been camouflaged its K_i shifting.

Therefore, is better by considering the proposals based on reduced random methods. These schemes can help us obtain too short the ciphertext and fast encryption process, without to put in risk the data security of the organisations. Although these alternatives can present low risk for the theft of digital data because some noisy bigger proportion are inserted to the ciphertext.

The improvement of encryption times was obtained only with the *reduced random* methods. Despite the successful results, a problem common to all these techniques is that they do not permit to control the selected maximum value of random ordinals of the ASCII table. Hence, can occur that some obtained random values will be out of range and therefore the ASCII can become as another encoding characters (e.g., UTF-8). In this work, this situation was not observed due to the fact the *mod 95* and *mod 120* have been employed because they produce sequences with allowed values in range of the ASCII table.

However, a selected plaintext in our experiments, it contains the '▓' character out of range of the ASCII table which has not been hidden with traditional Caesar proposals and this situation could not be controlled since data input. Therefore, if we observe in Table 1, only random Caesar and reduced random methods can hide these problems.

On the other hand, a modification of the ciphertext by dynamical methodologies here presented might be of interest. In particular, those that combines the simultaneous random noised selection with artificial

intelligence based on 1-NN rule and *pseudo-hexadecimal* or hexadecimal encoding. This involves a great variety of possibilities that we will cover in the next future work.

CONCLUSIONS

The updating of encryption methodologies periodically is one of the factors with a great influence on the performance of some cybersecurity strategies. Several works have been involved with the problems produced by the presence of the vulnerable encryption measures (e.g., if method is well known will become in inadequate). Therefore, in some papers (Álvarez 2019; Barranco and Galindo 2022; Delman 2004; Fulgueira et al. 2015; Gómez et al. 2012; Javidi et al. 1997; Linfei and Daomu 2005; Luciano and Prichett 1987; Mendoza 2008; Pisarchik and Zanin 2008; Rajan and Saumitr 2006; Rangel et al. 2023; Rangel et al. 2024; Reddaiah 2019; Rodríguez 2020; Rueda et al. 2005; William 1999) novel encryption alternatives have been recommended. In previous research (Rangel et al. 2023), some methodologies for handling to the usage of novel dynamical encryption methods have been experimented. Hence, this paper presents two modifications of these methodologies, for using it in those real applications of the organisations. Therefore, reduced and mutation random methods offer an important contribution to amend deficiencies of the available encryption strategies and to increase its usefulness. Experimental results with reduced and mutation random encryption methodologies have revealed that can cope with the data security problem with high levels of trust. These schemes allow the generalized results even greater than those obtained with the traditional *Caesar* algorithm. We intend to do further research on this issue. One of the techniques that we are going to explore is the employment of some measures for noised injection to the ciphertext based on reduced random schemes with the combined 1-NN rule and *pseudo-hexadecimal* format.

Tab.1. *The calculation of encryption/decryption times (in milliseconds) and estimated error are here shown. The columns A and B, are the average and standard deviation values, respectively. The ciphertext results for each encryption method are shown too. Two experimental tests with the same plaintext: "we will▒ meet at Midnight▒", different results have been obtained.*

	Ciphertext		Encryption time		Decryption time		% Error	
Encryption method	**Test 1**	**Test 2**	A	B	A	B	A	B
Traditional Caesar (by substitution)	ai ampp▓ qiix ex Qmhrmklx▓	ai ampp▓ qiix ex Qmhrmklx▓	2.4133	0.0198	2.3758	0.0213	0	0
Traditional Caesar (by shifting of K)	AI AMPP▓ QIIX EX QMHRMKLX▓	AI AMPP▓ QIIX EX QMHRMKLX▓	5.7221	0.0310	5.6651	0.0290	1	0
Random Caesar I	€ 9€ g2g%5%x1xi0io 3ol0l▓0▓%5%m0mj5 jj5jv2v'7'f5fv2v4U8 Up7pj6jq3qp7pm6mi1 it0t¯1¯	y2ym8m#3#~7~o6oo3 oo3o▙6▙"2"r5rn9nk6k }9}4e4ex4x 0 R5Rq8qf2fs5sj1ji2in6n u1u¯1¯	0.7997	0.0082	0.7888	0.0089	0	0
Random Caesar II (mod 95)	ÛdÛÌgÌR2Rš #š âyâ¦:¦ É]É℟ u℟ uUuºMºÔoÔ ” /” °<°S3S • • §3§{[{·j·×n×ÞzÞåwå Ÿ6Ÿš 3š ¥=¥¥1¥◂2◂	«4«ÆaÆˆ hˆ ¯8¯ž 5ž ÅYÅ¤8¤ʢwʢ}]}é|éÅ` Åá|á• !• ž ~ž ¨G¨×c×J *Jy,yÉ`É«G«¤6¤áxáÑj ÑÔlÔÁMÁ◍:◍	0.6810	0.0072	0.2261	0.0042	0	0
Random Caesar II (mod 120)	ìuì¢=¢S3S¤- ¤¬C¬ • ! • Ÿ3Ÿ◓ @◓ — w—ÜoÜõ • õÈcÈ§3§Š j Š %ɋ%ǾiÝ@ @Ì • ÌÌcÌ¹U¹ñƒ ñ¾U¾ã| ãû“ ûÖbÖ✟ • ✟	¥.¥ßzßcCcÒ[ÒÇ^ÇÔh ÔÍaÍ◊7◊” t” ³F³·R·’ - ’ ânâ£ƒ £ÄcÄéuéD$ Du(u«B«ÅaÅüŽ üÑh ÑŠ #Š æ~æÎZÎ☐}☐	0.6723	0.0105	0.2247	0.0021	0	0
Reduced random Caesar	àiŠ %‰ìàiÆ]ÕiÕiA Z ˆ hÖi²M±LÝi‰ˆ 'Ë W‰ì²eÒiœ8¥7ÒiÐiÑ i»G▮ i	Õ^ªE† f¿H˜ /·KÕi◩V sSÖi‘ ,ÎiÝi‰ì • < ,iIq$› 2Ã_ÄVÂY‘ * ÑiÝi☐h	**0.5678**	0.0088	**0.1972**	0.0026	0	0
Reduced random mutation	ài%Š ‰ìàiÆ]iÕÕiZ A ˆ hiÖ²ML±Ýii‰ˆ ' WË‰ìe²Òi8œ¥7iÒÐi iÑ»Gi▮	Õ^Eª† fH¿˜ /K·ÕiV◩ sSiÖ‘ ,iÎÝii‰• <, iI$q› 2_ÃÄVYÂ‘ *i ÑÝih☐	0.5723	0.0382	0.2024	0.0215	0	0
Average			**1.63**	**0.0177**	**1.38**	**0.0128**	**0.14**	**0**

REFERENCES

[1] Delman, B. 2004. "Genetic Algorithms in Cryptography". Thesis for the Degree of Master of Science in Computer Engineering. Rochester Institute of Technology, RIT Scholar Works. Department of Computer Engineering. Available at: https://scholar.google.com.mx/scholar_url?url=https://repository.rit.edu/cgi/viewcontent.cgi%3Farticle%3D6460%26context%3Dtheses&hl=es&sa=X&ei=cbaZZoadNt246rQPnd604AU&scisig=AFWwaeaMfCM5ORUFQN6DU4LA3aEG&oi=scholarr.

[2] Kalsi, S., Kaur, H., and Chang, V. 2018. "DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation". Convergence of Deep Machine Learning and Nature Inspired Computing Paradigms for Medical Informatics. Image & Signal Processing. In Journal of Medical Systems, volume 42. Article number: 17. DOI: https://doi.org/10.1007/s10916-017-0851.

[3] Mendoza, JC. 2008. "Demostración De Cifrado Simetrico Y Asimetrico". Ingenius. Revista de Ciencia y Tecnología, núm. 3, pp. 46-53. Universidad Politécnica Salesian. Cuenca, Ecuador. ISSN: 1390-650X. Available at: http://www.redalyc.org/articulo.oa?id=505554806007.

[4] Rangel, E., Rangel, KU., Medrano, J., Bernal, CA., and González, L. 2023. "Algoritmo Genético Para Cifrado De Datos, Basado En Un Nuevo Concepto Pseudo-Hexadecimal Con Inteligencia Artificial". Tecnológico Nacional De México, Instituto Tecnológico de Cd. Altamirano. Sexto (VI) Congreso Nacional De Investigación En Ciencia E Innovación De Tecnologías Productivas. Noviembre, 2023. Cd. Altamirano, Estado De Guerrero, México. Available at: https://www.cdaltamirano.tecnm.mx/index.php/17-vi-congreso-nacional-de-investigacion-en-ciencia-e-innovacion-de-tecnologias-productivas/140-tecnm-40 .

[5] Reddaiah, BA. 2019. "Study on Genetic Algorithms for Cryptography". International Journal of Computer Applications (0975 – 8887). Volume 177 - No. 28, December 2019. Department of Computer Applications. Yogi Vemana University Kadapa, A.P, India. Available at: https://www.researchgate.net/publication/338012809_A_Study_on_Genetic_Algorithms_for_Cryptography .

[6] Rangel, E., Campos, M., Rangel, KU., González, L., and Medrano, J. (2024). "La Regla Del Vecino Más Cercano Inyectando Ruido Hexadecimal A Mensajes Encriptados Para Seguridad De Datos En Las Organizaciones". Send to: LATAM: Revista Latinoamericana de Ciencias Sociales y Humanidades. Asunción, Paraguay. ISSN en línea: 2789-3855, (2024), Volumen 5, Número 2, p 1.

[7] Sebas, C. 2023. "¿Qué son los Algoritmos Genéticos en las Inteligencias Artificiales?". Manuales y Tutoriales de Informatica. Available at: https://aprendeinformaticas.com/ia/ .

[8] Barranco, F., and Galindo, C. 2022. "Criptografía básica y algunas aplicaciones". Universidad Jaume I, Departamento de Matemáticas, Castellón, España. Available at: https://repositori.uji.es/xmlui/bitstream/handle/10234/201359/TFM_2022_Barranco_Bl%C3%A1zquez_FranciscoMiguel.pdf?sequence=1 .

[9] Gómez, S. , Arias, JD., and Agudelo, D. 2012. "Cripto-Análisis Sobre Métodos Clásicos De Cifrado". Scientia Et Technica, vol. XVII, núm. 50, abril, pp. 97-102. Universidad Tecnológica de Pereira Pereira, Colombia. ISSN 0122-1701 97. Available at: http://www.redalyc.org/articulo.oa?id=84923878015.

[10] Javidi, B., Zhang, GS., and Li, J. 1997. "Encrypted Optical Memory Using Double-random Phase Encoding". Appl. Opt. 36, 1054-1058. Available at: https://pubmed.ncbi.nlm.nih.gov/18250772/ .

[11] Cover, TM., and Hart, PE. 1967. "Nearest Neighbor Pattern Classification". IEEE Transactions on Information Theory, Volume IT-13, January 1967, pages 21-27. Available at: https://ieeexplore.ieee.org/abstract/document/1053964/.

[12] Barandela, R., Sánchez, JS., García, V., and Rangel, E. 2003. "Strategies for Learning in Class Imbalance Problems". Pattern Recognition, Vol. 36, No. 3, pp. 849-851. Rapid and Brief Comunication (Pergamon) ISBN: (PII: S0031-3203(02)00257-1. 0031-3203/02/). Available at: https://doi.org/10.1016/S0031-3203(02)00257-1 .

[13] Rangel, E. 2022. "La Regla De Los k Vecinos Más Cercanos (k-NN) Basada En Distancia De Manhattan (City-Block) Para Mejorar La Clasificación De Patrones". Publicado En: Quinto Congreso Nacional De Investigación En Ciencia E Innovación De Tecnologías Productivas. Tecnológico Nacional De México (campus: Instituto Tecnológico de Cd. Altamirano). Noviembre, 2022. Cd. Altamirano, Estado De Guerrero, México. Available at: http://erangel.coolpage.biz/pappers/edgarrangel2022.pdf .

[14] Álvarez, D. 2019. "Algunos Aspectos Jurídicos Del Cifrado De Comunicaciones". Derecho PUCP, núm. 83, 2019, pp. 241-264. Pontificia Universidad Católica del Perú (2019). DOI: https://doi.org/10.18800/derechopucp.201902.008. Available at: http://www.redalyc.org/articulo.oa?id=533662765008.

[15] Fulgueira, M., Hernández, OA., and Henry, V. 2015. "Paralelización Del Algoritmo Criptográfico GOST Empleando El Paradigma De Memoria Compartida". Lámpsakos, núm. 14, pp. 18-24. Fundación Universitaria Luis Amigó Medellín, Colombia. E-ISSN: 2145-4086; julio-diciembre 2015. DOI: http://dx.doi.org/10.21501/21454086.1633. Available at: http://www.redalyc.org/articulo.oa?id=613965326004.

[16] Luciano, D., and Prichett, G. 1987. "Cryptology: From Caesar Ciphers To Public-key Cryptosystems". The College Mathematics Journal, vol 18 pp 2-17. Available at: http://www.jstor.org/stable/2686311 .

[17] Linfei, C., and Daomu, Z. 2005. "Optical Image Encryption Based On Fractional Wavelet". Transform, Opt. Comm. Vol. 254, p.p. 361-367. Available at: https://ui.adsabs.harvard.edu/abs/ 2005OptCo.254..361C/abstract .

[18] Pisarchik, AN., and Zanin, M. 2008. "Imagen Encryption Witch Chaotically Coupled Chaotic Maps". Elsevier Physica, D 237, abril 2008 [en línea]. Available at: www.elsevier.com/locate/physd.

[19] Rajan, B., and Saumitr, PA. 2006. "Novel Compression And Encryption Scheme Using Variable Model Arithmetic Coding And Coupled Chaotic System". IEEE Transactions on circuits and system- I, volumen 53 (número 4), abril 2006. Available at: https://www.researchgate.net/publication/3451216_A_novel_compression_and_encryption_scheme_using_variable_model_arithmetic_coding_and_coupled_chaotic_system

[20] Rueda, JE., Romero, AL., and Castro, LM. 2005. "Criptografía Digital Basada En Tecnología Óptica". Bistua: Revista de la Facultad de Ciencias Básicas, vol. 3, núm. 2, julio 2005, pp. 19-25. ISSN 0120 - 4211. Universidad de Pamplona, Colombia. Available at: http://www.redalyc.org/articulo.oa?id=90330203.

[21] William, S. 1999. "Cryptography and Network Security: Principles and Practice 2nd edition". Prentice-Hall, Inc., pp 23-50. Available at: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf&ved=2ahUKEwjXsIql8rGHAxWsKUQIHTA-APIQFnoECBQQAQ&usg=AOvVaw2IROGmmRSXMbAjzdVHzwug

[22] Rodríguez, J. 2020. "Operadores Genéticos Aplicados A La Criptografía Simétrica". Proyecto De Grado. Universidad Distrital Francisco José De Caldas. Facultad De Ingeniería. Ingeniería De Sistemas. Bogotá, Colombia. Available at: https://repository.udistrital.edu.co/handle/11349/28192 .

[23] Progress Software Corporation, Telerik. 2022. "Cifrado Y Transferencia De Archivos: Los Mejores Cifrados Seguros Para La Transferencia De Archivos". Ipswitch Blogs (2020-2022). Access/Revisión: 31-08-2024. Available at: https://ipswitch.com/amp/es/los-mejores-cifrados-seguros-para-la-transferencia-de-archivos/.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 92 – 111 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CYBERSECURITY: EMERGING TRENDS AND CHALLENGES

Habib Badawi[1]
[1]Lebanese University, Beirut, Lebanon

ABSTRACT: This comprehensive study explores the multifaceted landscape of cybersecurity, integrating technical, human, ethical, and international perspectives. Drawing on a robust theoretical framework, we examine emerging trends in threat intelligence, critical infrastructure protection, the human factor in cybersecurity, ethical considerations, and international cooperation. Our findings highlight the need for a holistic approach to cybersecurity that balances technological solutions with human-centric strategies, ethical considerations, and global collaboration. The study provides insights for policymakers, cybersecurity professionals, and researchers, offering a roadmap for navigating the complex and evolving cybersecurity terrain.

KEYWORDS: Cybersecurity, Threat Intelligence, Human Factors, Ethics, International Cooperation, Critical Infrastructure, Cyber Resilience.

METHODOLOGY: This study employed a qualitative research approach, combining an extensive literature review with theoretical analysis. We synthesized findings from peer-reviewed academic journals, government reports, and industry white papers. The theoretical framework was constructed by integrating multiple theories and models relevant to cybersecurity, including Socio-Technical Systems Theory, Protection Motivation Theory, and the NIST Cybersecurity Framework. This interdisciplinary approach allowed for a comprehensive examination of cybersecurity from technical, human, ethical, and international perspectives.

NOVELTY AND CONTRIBUTIONS:

1. **Ethical Considerations: The** incorporation of an ethical framework for cybersecurity addresses a critical gap in many technical-focused cybersecurity studies, highlighting the importance of balancing security measures with privacy and individual rights.
2. **Human-Centric Perspective:** By emphasizing the role of human factors and proposing a shift from viewing humans as the "weakest link" to potential "security heroes," the study contributes to the evolving discourse on human-centric cybersecurity.
3. **Integrated Theoretical Framework:** The study presents a novel, comprehensive theoretical framework that combines technical, behavioral, ethical, and international cooperation models, providing a holistic lens for understanding cybersecurity challenges.
4. **Interdisciplinary Approach:** By bridging technical, social, ethical, and policy perspectives, the study offers a unique interdisciplinary view of cybersecurity challenges and solutions.
5. **International Cooperation Model:** The study emphasizes the global nature of cyber threats and proposes a model for international cooperation, contributing to the ongoing dialogue on global cybersecurity governance.

Classification Codes: ACM Computing Classification System:

- Security and privacy → Human and societal aspects of security and privacy
- Security and privacy → Network security
- Social and professional topics → Computing / technology policy

JEL Classification:

- O33 Technological Change: Choices and Consequences; Diffusion Processes
- K24 Cyber Law
- F52 National Security and Economic Nationalism

THEORETICAL FRAMEWORK

This study's theoretical framework is built upon several interconnected theories and models that collectively address the multifaceted nature of cybersecurity:

1. **Cybersecurity Capability Maturity Model (C2M2):** Developed by the U.S. Department of Energy (2014), this model provides a framework for assessing and improving cybersecurity capabilities, particularly in critical infrastructure sectors.
2. **Ethical Framework for Cybersecurity:** Drawing from the work of Taddeo and Floridi (2018), this component of our framework addresses the ethical implications of cybersecurity measures, including privacy concerns and the potential for abuse of security technologies.
3. **Human-Centric Security Model:** Building on the work of Pfleeger et al. (2014), this model shifts the perspective from viewing humans as the "weakest link" to potential "security heroes," emphasizing the importance of human factors in cybersecurity.
4. **International Cooperation Model:** Based on insights from Choo (2011) and initiatives like the Budapest Convention on Cybercrime (Council of Europe, 2001), this aspect of our framework addresses the necessity and challenges of international collaboration in addressing global cyber threats.
5. **NIST Cybersecurity Framework:** This framework, developed by the National Institute of Standards and Technology (2018), offers a risk-based approach to managing cybersecurity risk, emphasizing five core functions: Identify, Protect, Detect, Respond, and Recover.
6. **Protection Motivation Theory:** Originally developed by Rogers (1975) and applied to cybersecurity by Ifinedo (2012), this theory helps explain individual security behaviors. It suggests that people's motivation to protect themselves is influenced by their perception of threat severity, vulnerability, response efficacy, and self-efficacy.
7. **Socio-Technical Systems Theory:** This theory, as applied by Soomro et al. (2016), forms the foundation of our framework. It posits that effective cybersecurity requires the integration of both technical and social elements, emphasizing the need for a holistic approach that considers technology, people, processes, and organizational factors.
8. **Theory of Planned Behavior**: This theory, utilized by Safa et al. (2016) in the context of information security policy compliance, provides insights into how attitudes, subjective norms, and perceived behavioral control influence individuals' intentions to engage in secure behaviors.

This integrated theoretical framework provides a comprehensive lens through which to examine the complex interplay of technical, human, organizational, ethical, and international factors in cybersecurity.

1. INTRODUCTION

In an increasingly interconnected world, cybersecurity has become a critical concern for individuals, organizations, and nations. As cyber threats evolve in complexity and scale, traditional security measures are often found wanting. This paper explores recent developments in cybersecurity, with a particular focus on threat intelligence, critical infrastructure protection, the human elements of cybersecurity, ethical considerations, and international cooperation.

The rapid digitalization of society has created new vulnerabilities and expanded the attack surface for malicious actors. From nation-state sponsored cyber-attacks to individual hackers, the threats are diverse and ever-changing. As Choo (2011) notes, "The cyber threat landscape is complex and dynamic, with threats emerging from various sources, including organized crime groups, hacktivists, and state-sponsored actors" (p. 720). This complexity necessitates a multifaceted approach to cybersecurity that goes beyond mere technical solutions.

The importance of cybersecurity cannot be overstated. It is fundamental to the functioning of modern society, from protecting critical infrastructure to safeguarding personal data. As our reliance on digital technologies grows, so does the potential impact of cyber-attacks. The NotPetya malware attack of 2017, for instance, caused global damage estimated at $10 billion, highlighting the far-reaching consequences of cyber threats (Lallie et al., 2021).

This paper aims to provide a comprehensive overview of the current state of cybersecurity, focusing on five key areas:

1. **Critical Infrastructure Protection:** The paper will examine strategies for protecting vital systems and networks that underpin national security and economic stability.
2. **Ethical Considerations:** The paper will discuss the ethical implications of cybersecurity measures, including privacy concerns and the potential for abuse of security technologies.
3. **International Cooperation:** We will examine the importance of global collaboration in addressing cyber threats that transcend national boundaries.
4. **The Human Factor:** We will delve into the crucial role that human behavior plays in cybersecurity and explore strategies for improving security awareness and practices.
5. **Threat Intelligence:** We will explore the latest developments in threat intelligence, including the use of automation and artificial intelligence in detecting and responding to threats.

By examining these interconnected aspects of cybersecurity, this paper aims to provide a holistic view of the challenges and opportunities in this rapidly evolving field.

2. THREAT INTELLIGENCE: CURRENT STATE AND FUTURE DIRECTIONS

Threat intelligence has emerged as a critical component of modern cybersecurity strategies. It involves the collection, analysis, and dissemination of information about potential or current attacks that threaten an organization's assets. As cyber threats become more sophisticated, the need for robust threat intelligence capabilities has never been greater.

Current State

The SANS 2020 Cyber Threat Intelligence (CTI) Survey provides valuable insights into the current state of threat intelligence practices (SANS Security Insights et al., 2020). The survey reveals that while many organizations recognize the importance of threat intelligence, there are still significant challenges in its implementation and utilization.

One key finding is the growing emphasis on automation in threat intelligence processes. Organizations are increasingly turning to automated tools to collect, analyze, and disseminate threat intelligence, allowing for more rapid response to emerging threats. However, the survey also highlights the continued importance of human analysts in interpreting and contextualizing threat data.

The integration of threat intelligence into existing security operations remains a challenge for many organizations. According to the SANS survey, only 41% of respondents reported that their organization's CTI was fully integrated with their security operations. This suggests a significant opportunity for improvement in how threat intelligence is leveraged to enhance overall security posture.

Future Directions

The future of threat intelligence lies in real-time, actionable insights that can be seamlessly integrated into an organization's security operations. Cybersixgill (n.d.) emphasizes the need for real-time, actionable threat intelligence. Their approach focuses on leveraging dark web sources to provide early warning of potential threats, illustrating the expanding scope of threat intelligence gathering.

Artificial Intelligence (AI) and Machine Learning (ML) are set to play an increasingly key role in threat intelligence. These technologies can help process vast amounts of data, identify patterns, and predict potential threats more quickly and accurately than human analysts alone. As Nurse et al. (2017) note, "AI and ML techniques can significantly enhance the ability to detect and respond to cyber threats in real-time" (p. 22). Another emerging trend is the use of threat intelligence platforms (TIPs) that aggregate and analyze data from multiple sources. These platforms can provide a more comprehensive view of the threat landscape and help organizations prioritize their security efforts more effectively.

The future of threat intelligence also involves a greater focus on proactive threat hunting. Rather than waiting for alerts to be triggered, security teams are actively searching for hidden threats within their networks. This approach, combined with advanced analytics, can help organizations detect and respond to threats more quickly.

However, as threat intelligence capabilities advance, so do the tactics of cyber attackers. The arms race between defenders and attackers is likely to intensify, with each side developing more sophisticated tools and techniques. This underscores the need for continuous innovation and adaptation in the field of threat intelligence.

3. CRITICAL INFRASTRUCTURE PROTECTION

The protection of critical infrastructure is a cornerstone of national cybersecurity strategies. Critical infrastructure refers to the systems and assets that are essential for the functioning of society and the economy. The U.S. Department of Homeland Security (2019) identifies 16 critical infrastructure sectors, including energy, healthcare, and financial services, which are essential to national security and economic stability.

The importance of protecting these sectors cannot be overstated. A successful cyber-attack on critical infrastructure could have devastating consequences, potentially disrupting essential services, causing economic damage, and even threatening human lives. The 2015 Ukraine power grid attack, which left 230,000 people without electricity, serves as a stark reminder of the potential impact of such attacks (Denning, 2011).

Framework for Improving Critical Infrastructure Cybersecurity

Recognizing the need for a standardized approach to critical infrastructure protection, the National Institute of Standards and Technology (NIST) developed the Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018). This framework provides a risk-based approach to managing cybersecurity risk, emphasizing the importance of continuous assessment and improvement.

The NIST framework is built around five core functions:

1. **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
2. **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
3. **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
4. **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

5. **Respond:** Develop and implement appropriate activities to act regarding a detected cybersecurity incident.

This framework provides a flexible and adaptable approach that can be tailored to the specific needs and risk profiles of different organizations and sectors. Its emphasis on continuous improvement is particularly important given the rapidly evolving nature of cyber threats.

Case Studies

Several case studies illustrate both the challenges and successes in critical infrastructure protection:

1. **Energy Sector:** The 2015 Ukraine power grid attack mentioned earlier highlighted the vulnerability of energy infrastructure to cyber-attacks. In response, many countries have implemented more robust cybersecurity measures for their power grids. For instance, the U.S. Department of Energy has developed the Cybersecurity Capability Maturity Model (C2M2) to help energy sector organizations evaluate and improve their cybersecurity capabilities (U.S. Department of Energy, 2014).
2. **Financial Services:** The financial sector has long been a prime target for cyber-attacks due to the potential for financial gain. The 2016 Bangladesh Bank heist, where cybercriminals attempted to steal $1 billion, highlighted the need for robust cybersecurity in the financial sector. In response, many financial institutions have implemented advanced threat detection systems and improved their incident response capabilities (Holt et al., 2018).
3. **Healthcare Sector:** The healthcare sector has become an increasingly attractive target for cybercriminals, particularly with the rise of ransomware attacks. The WannaCry ransomware attack in 2017 affected numerous healthcare organizations globally, including the UK's National Health Service (NHS). This incident led to significant improvements in cybersecurity practices in the healthcare sector, including better patch management and increased investment in cybersecurity infrastructure (Lallie et al., 2021).

These case studies underscore the importance of sector-specific approaches to critical infrastructure protection. While the NIST framework provides a general guideline, each sector faces unique challenges that require tailored solutions.

Challenges and Future Directions

Despite progress in critical infrastructure protection, significant challenges remain. These include:

1. **Insider Threats:** While much focus is placed on external threats, insider threats – whether malicious or unintentional – pose a significant risk to critical infrastructure. Addressing this challenge requires a combination of technological solutions and human-focused strategies (Greitzer et al., 2014).
2. **Interdependencies:** Critical infrastructure sectors are increasingly interconnected, meaning that a disruption in one sector can have cascading effects on others. Understanding and managing these interdependencies is crucial for effective protection.
3. **Legacy Systems:** Many critical infrastructure systems rely on legacy technology that was not designed with cybersecurity in mind. Upgrading these systems can be costly and complex, leaving vulnerabilities that can be exploited by attackers.
4. **Supply Chain Risks:** The global nature of supply chains introduces additional risks, as vulnerabilities in one part of the chain can impact the entire system. Managing these risks requires a comprehensive approach that extends beyond an organization's immediate boundaries.

Looking to the future, emerging technologies such as 5G networks and the Internet of Things (IoT) are set to transform critical infrastructure, bringing both new opportunities and new risks. As Nurse et al. (2017) point out, "The proliferation of IoT devices in critical infrastructure introduces new attack vectors that need to be carefully managed" (p. 21).
Addressing these challenges will require ongoing collaboration between government agencies, private sector organizations, and cybersecurity experts. It will also necessitate continued investment in research and development to stay ahead of evolving threats.

4. THE HUMAN FACTOR IN CYBERSECURITY

While technological solutions are crucial, the human element remains a critical factor in cybersecurity. As Soomro et al. (2016) note, "The human factor is often considered the weakest link in the information security chain" (p. 216). However, recent research suggests that this perspective may be overly simplistic and that humans can also be a strong line of defense when properly educated and motivated.

Transformative Approaches

Pfleeger et al. (2014) argues for a transformative approach to staff security behavior, moving from viewing employees as the "weakest link" to potential "security heroes." Their research emphasizes the importance of understanding human behavior and motivation in designing effective security policies and training programs. This approach recognizes that employees can be an asset in detecting and preventing security breaches when they are properly engaged and empowered.
Schneier (2000) further explores the human aspects of security in his seminal work "Secrets and Lies: Digital Security in a Networked World." He argues that true security requires a holistic approach that considers not just technology, but also people and processes. Schneier emphasizes the importance of understanding the psychology of security and how human behavior both can enhance and undermine security measures.

Understanding Human Behavior in Cybersecurity

To effectively address the human factor in cybersecurity, it is crucial to understand the underlying psychological and behavioral factors that influence security-related decisions and actions. Several key areas have been identified in the literature:

1. **Cognitive Biases:** Various cognitive biases can influence security behavior. For example, the optimism bias can lead individuals to underestimate their own vulnerability to cyber threats (Waly et al., 2012).
2. **Decision-Making Under Uncertainty:** Cybersecurity often involves making decisions in uncertain and complex environments. Hadlington (2017) explored the link between impulsivity and risky cybersecurity behaviors, finding that individuals with higher levels of impulsivity were more likely to engage in behaviors that could compromise security.
3. **Risk Perception:** How individuals perceive and evaluate cyber risks can significantly impact their security behavior. Ifinedo (2012) found that individuals' perception of the severity of security threats and their own vulnerability to these threats were significant predictors of their intention to comply with information security policies.
4. **Social Influence:** The behavior of colleagues and superiors can have a significant impact on an individual's security practices. Safa et al. (2016) found that social bonds within an organization were positively associated with information security policy compliance.

Security Awareness and Training

Effective security awareness and training programs are crucial in addressing the human factor in cybersecurity. However, traditional approaches to security training have often been criticized as ineffective and uninspiring. Bada et al. (2019) argue that many security awareness campaigns fail to change behavior because they focus on providing information rather than addressing the underlying factors that influence behavior.

To address these shortcomings, several innovative approaches have been proposed:

1. **Continuous Learning:** Rather than one-off training sessions, continuous learning approaches can help reinforce security concepts and keep employees updated on emerging threats. Furnell and Thomson (2009) emphasize the importance of regular reinforcement to combat "security fatigue" and maintain vigilance.
2. **Gamification:** Incorporating game elements into security training can increase engagement and retention. Conklin (2006) demonstrated the effectiveness of cyber defense competitions in enhancing students' cybersecurity skills and awareness.
3. **Personalized Training:** Tailoring security training to individual roles and risk profiles can increase its relevance and effectiveness. Torten et al. (2018) found that role-based security training was more effective in improving security behavior than general awareness programs.
4. **Storytelling:** Using narratives and real-world examples can make security concepts more relatable and memorable. Aloul (2010) suggests using case studies of actual security incidents in training programs to illustrate the potential consequences of poor security practices.

Combating Social Engineering

Social engineering attacks, which exploit human psychology to gain unauthorized access to systems or information, represent a significant challenge in cybersecurity. As Krombholz et al. (2015) note, "Social engineering attacks are becoming increasingly sophisticated and difficult to detect" (p. 114).

Addressing this challenge requires a multifaceted approach:

1. **Cultural Change:** Fostering a security-conscious culture where employees feel comfortable reporting suspicious activities is crucial in combating social engineering threats.
2. **Education:** Employees need to be trained to recognize common social engineering tactics, such as phishing emails and pretexting.
3. **Simulation:** Regular simulated social engineering attacks can help employees practice their response and identify areas for improvement.
4. **Technical Controls:** While not a complete solution, technical controls such as email filters and multi-factor authentication can provide an additional layer of defense against social engineering attacks.

Future Directions

As technology continues to evolve, so will the human factors in cybersecurity. Emerging technologies such as artificial intelligence and machine learning are likely to change the nature of human-computer interaction in security contexts. Oltramari et al. (2015) suggest that developing a comprehensive human factors ontology for cybersecurity could help in better understanding and addressing the complex interplay between human behavior and technological systems. Moreover, as remote work becomes increasingly common, new

challenges in managing human-related security risks are likely to emerge. This may necessitate innovative approaches to security awareness and training that are better suited to distributed workforces.

5. ETHICAL CONSIDERATIONS IN CYBERSECURITY

As cybersecurity measures become more sophisticated, they also raise important ethical questions. Taddeo and Floridi (2018) explore the ethics of cybersecurity, discussing issues such as privacy, autonomy, and the potential for abuse of cybersecurity technologies. They argue for the need to balance security imperatives with ethical considerations and human rights.

Privacy vs. Security

One of the central ethical dilemmas in cybersecurity is the tension between privacy and security. While robust security measures often require extensive monitoring and data collection, this can infringe on individual privacy rights. As Luo et al. (2011) note, "The challenge lies in finding the right balance between protecting organizational assets and respecting individual privacy" (p. 3).
This dilemma is particularly acute in the context of government surveillance programs. The revelations by Edward Snowden in 2013 about the extent of NSA surveillance sparked a global debate about the ethics of mass surveillance in the name of national security. These debates highlight the need for transparent and accountable cybersecurity practices that respect individual rights while still providing adequate protection against threats.

Autonomy and Informed Consent

Another key ethical consideration is the impact of cybersecurity measures on individual autonomy. As security systems become more pervasive and automated, there is a risk that they could unduly restrict individual freedom and decision-making. This raises questions about informed consent: to what extent should individuals be aware of and have control over the security measures that affect them?
This issue is particularly relevant in the context of workplace monitoring. While organizations have a legitimate interest in protecting their assets, overly intrusive monitoring can create a culture of distrust and potentially violate employee privacy rights. Striking the right balance requires careful consideration of both security needs and ethical principles.

Ethical Hacking and Vulnerability Disclosure

The practice of ethical hacking, where security professionals attempt to breach systems to identify vulnerabilities, raises its own set of ethical questions. While this practice can help improve security, it also involves intentionally exploiting vulnerabilities, which could be seen as unethical if not conducted with proper authorization and safeguards.
Related to this is the issue of vulnerability disclosure. When researchers discover security flaws, they face ethical dilemmas about how and when to disclose this information. Immediate public disclosure could put users at risk if a fix is not available, but delaying disclosure could leave vulnerabilities unaddressed. As Holt et al. (2018) discuss, "Responsible disclosure policies aim to balance the need for transparency with the imperative to protect users from potential harm" (p. 287).

Artificial Intelligence and Automation in Cybersecurity

The increasing use of AI and automation in cybersecurity raises new ethical concerns. While these technologies can greatly enhance security capabilities, they also introduce risks of bias, lack of

transparency, and potential loss of human control. Taddeo and Floridi (2018) argue that "the use of AI in cybersecurity must be guided by clear ethical principles to ensure it respects human rights and democratic values" (p. 5).

One particular concern is the potential for AI-powered security systems to perpetuate or exacerbate existing biases. If training data or algorithms reflect societal biases, this could lead to unfair or discriminatory security practices. Ensuring fairness and transparency in AI-driven security systems is thus a critical ethical imperative.

Global Perspectives on Cybersecurity Ethics

It is important to note that ethical considerations in cybersecurity can vary across diverse cultural and legal contexts. What may be considered an acceptable trade-off between security and privacy in one country might be viewed as unethical in another. This global diversity of perspectives adds another layer of complexity to cybersecurity ethics, particularly for multinational organizations and in the context of international cybersecurity cooperation.

As cybersecurity continues to evolve, ongoing ethical reflection and debate will be crucial. Developing ethical frameworks and guidelines for cybersecurity practices, such as those proposed by Taddeo and Floridi (2018), can help navigate these complex issues and ensure that cybersecurity measures align with broader societal values and human rights principles.

6. INTERNATIONAL COOPERATION AND CYBERSECURITY STRATEGY

Given the global nature of cyber threats, international cooperation is essential for effective cybersecurity. As Choo (2011) notes, "Cybercrime and cyber-attacks often transcend national boundaries, necessitating international collaboration in both prevention and response" (p. 725). This section explores the challenges and opportunities in international cybersecurity cooperation, as well as key strategies and policies.

Challenges in International Cooperation

Several factors complicate international cooperation in cybersecurity:

1. **Attribution Difficulties:** The anonymous nature of many cyber-attacks makes it challenging to definitively attribute them to specific actors, complicating international law enforcement efforts.
2. **Sovereignty and National Interests:** Nations may be reluctant to share sensitive information or cede control over their cybersecurity measures due to concerns about national sovereignty and security.
3. **Trust Issues:** Geopolitical tensions and competing national interests can erode trust between nations, making it difficult to establish effective cooperation mechanisms.
4. **Varying Legal Frameworks:** Different countries have different laws and regulations regarding cybercrime and data protection, which can hinder coordinated action.

International Initiatives and Agreements

Despite these challenges, there have been significant efforts to foster international cooperation in cybersecurity:

1. **Budapest Convention on Cybercrime:** This 2001 international treaty, ratified by over 60 countries, aims to harmonize national laws on cybercrime and improve international cooperation in cybercrime investigations (Council of Europe, 2001).

2. **UN Group of Governmental Experts (UN GGE): This** group has worked to develop norms of responsible state behavior in cyberspace and promote international law in the cyber domain (United Nations, 2015).
3. **Paris Call for Trust and Security in Cyberspace:** Launched in 2018, this multi-stakeholder initiative promotes nine common principles for securing cyberspace, including the protection of critical infrastructure and collaborative security (French Ministry for Europe and Foreign Affairs, 2018).

National Cybersecurity Strategies

Many countries have developed comprehensive national cybersecurity strategies to address the evolving threat landscape. The U.S. Department of Homeland Security's (2016) Cybersecurity Strategy emphasizes the importance of collaboration with international partners to address shared cyber risks. Key elements of this strategy include:

1. **Capacity Building:** Supporting the development of cybersecurity capabilities in partner nations to strengthen global resilience against cyber threats.
2. **Cyber Diplomacy:** Engaging in diplomatic efforts to promote responsible state behavior in cyberspace and develop international norms.
3. **Incident Response:** Improving coordination in responding to major cyber incidents that have international implications.
4. **Information Sharing:** Enhancing mechanisms for sharing threat intelligence and best practices with international partners.

Public-Private Partnerships

International cooperation in cybersecurity extends beyond government-to-government interactions. Public-private partnerships play a crucial role in addressing global cyber threats. As Soomro et al. (2016) point out, "Effective cybersecurity requires collaboration between governments, private sector organizations, and academic institutions across national boundaries" (p. 220).
Many multinational corporations have significant cybersecurity resources and expertise that can complement government efforts. Initiatives like the Cyber Threat Alliance, which brings together cybersecurity companies to share threat intelligence, demonstrate the potential of private sector cooperation in addressing global cyber threats (Cyber Threat Alliance, 2017).

Future Directions

As cyber threats continue to evolve, so must international cooperation efforts too. Several trends are likely to shape the future of international cybersecurity cooperation:

1. **AI and Emerging Technologies:** The rise of AI and other emerging technologies will create new challenges and opportunities for international cooperation. Developing shared norms and standards for the use of these technologies in cybersecurity will be crucial.
2. **Cyber Capacity Building:** There will likely be an increased focus on helping developing nations build their cybersecurity capabilities to create a more resilient global cyber ecosystem.
3. **Multi-stakeholder Approaches:** Future cooperation efforts are likely to increasingly involve a diverse range of stakeholders, including governments, private sector entities, civil society organizations, and academic institutions.
4. **Supply Chain Security:** Given the global nature of technology supply chains, international cooperation will be essential in addressing supply chain security risks.

As Lallie et al. (2021) note, "The COVID-19 pandemic has highlighted the critical importance of international cooperation in addressing global cyber threats" (p. 102250). This global crisis has accelerated digital transformation and exposed new cybersecurity vulnerabilities, underscoring the need for robust international collaboration in the cyber domain.

7. CONCLUSION: NAVIGATING THE COMPLEX LANDSCAPE OF CYBERSECURITY

This comprehensive study has illuminated the multifaceted and ever-evolving domain of cybersecurity, revealing a landscape that extends far beyond mere technological fixes. It presents itself as an intricate tapestry, woven with threads of technical challenges, human behaviors, ethical concerns, and the imperative for global cooperation. Our exploration has unveiled cybersecurity as a complex ecosystem, where innovation, moral imperatives, and international collaboration intersect in a delicate balance.

Key themes and insights

Throughout our analysis, several critical themes have emerged, each contributing to a holistic understanding of the cybersecurity landscape:

1. **Continuous Adaptation and Learning**: The cybersecurity landscape is a theater of constant evolution, where yesterday's solutions may become tomorrow's vulnerabilities. This reality calls for an approach deeply rooted in perpetual learning and adaptation. Echoing Schneier's (2000) sage observation that "security is not a product but a process" (p. 85), we recognize the imperative for ongoing education, training, and flexibility. This philosophy of continuous improvement must permeate every aspect of cybersecurity, from technological implementations to human resource development, ensuring that our defenses evolve in tandem with—or ideally, ahead of—emerging threats.
2. **Ethical Imperatives in the Digital Age**: As cybersecurity mechanisms grow increasingly sophisticated, they give rise to Pandora's box of ethical dilemmas. The Ethical Framework for Cybersecurity emerges as a moral compass, guiding practitioners through the labyrinth of conflicting demands between stringent security protocols and sacrosanct individual rights. This delicate balance act between robust protection and the preservation of privacy and autonomy is not a one-time achievement but an ongoing journey, demanding constant vigilance, reassessment, and ethical recalibration in the face of evolving threats and societal values.
3. **The Centrality of the Human Element**: While technological advancements form the backbone of cybersecurity, the human factor remains the heart and soul of effective defense strategies. Pfleeger et al. (2014) illuminates the pivotal challenge and opportunity of metamorphosing employee behavior from a potential Achilles' heel into a formidable security asset. The Human-Centric Security Model further reinforces this paradigm shift, urging us to view individuals not as liabilities but as invaluable sentinels in the cybersecurity fortress. This perspective transforms our approach from mere risk mitigation to empowerment, fostering a culture where every user becomes an active guardian of digital security.
4. **The Imperative of Integration**: Effective cybersecurity demands a seamless integration of diverse elements, akin to a symphony where each instrument plays a crucial role in creating a harmonious whole. As Soomro et al. (2016) aptly emphasize, "A holistic approach to information security management is essential for addressing the complex and dynamic nature of cyber threats" (p. 223). This integration spans the spectrum from threat intelligence and technological solutions to human factors, ethical considerations, and international cooperation. Frameworks such as the Cybersecurity Capability Maturity Model (C2M2) and the NIST Cybersecurity Framework serve as conductors in this intricate performance, providing structured methodologies to navigate the rapidly shifting terrain of cyber threats and defenses.

5. **The Necessity of Global Collaboration** In our interconnected digital world, cyber threats traverse borders with the fluidity of wind, rendering international collaboration not just beneficial but indispensable. The International Cooperation Model underscores a sobering truth: our collective cybersecurity defense is only as robust as its most vulnerable link. The path forward necessitates overcoming formidable barriers such as trust deficits, concerns over national sovereignty, and hesitancy in information sharing. Building robust global cybersecurity frameworks requires a level of international cooperation akin to global efforts against climate change or pandemics, where the security of one is inextricably linked to the security of all.

Theoretical Foundations and Practical Implications

Our study has been anchored in several theoretical frameworks, each offering profound insights into the multifaceted nature of cybersecurity:

The Socio-Technical Systems Theory serves as a reminder that cybersecurity is not a purely technological challenge but a human one as well. It emphasizes the need for organizations to maintain a delicate equilibrium between cutting-edge technology and the people who interact with these systems. This theory underscores the importance of considering organizational culture, user behavior, and social dynamics in designing and implementing cybersecurity measures.

The Protection Motivation Theory and the Theory of Planned Behavior offer crucial insights into the labyrinth of human decision-making when faced with cyber threats. These frameworks illuminate the cognitive processes underlying risk perception and response, providing a roadmap for effective behavior modification strategies. By understanding the psychological factors that influence security-related decisions, organizations can design more effective training programs and security policies that resonate with users on a deeper level.

The Cybersecurity Capability Maturity Model (C2M2) and the NIST Cybersecurity Framework stand as beacons, offering structured approaches to assess and enhance an organization's cybersecurity posture. These models provide practical tools for navigating the complex cybersecurity landscape, enabling organizations to benchmark their current practices, identify gaps, and chart a course for continuous improvement. By offering a common language and set of standards, these frameworks facilitate better communication and collaboration both within and between organizations.

Future Directions and Research Opportunities

As we gaze into the horizon of cybersecurity, several key areas emerge as fertile ground for further exploration and innovation:

The impact of emerging technologies such as quantum computing, 5G networks, and advanced AI systems looms large on the cybersecurity landscape. These technologies promise to revolutionize our digital infrastructure, but they also bring unprecedented challenges. Research is urgently needed to understand how these technologies will reshape the threat landscape and to develop novel defense mechanisms that can withstand the test of quantum supremacy and AI-powered attacks.

The realm of cybersecurity education and training stands as a critical frontier. Developing more effective methods for cultivating cybersecurity awareness and skills is paramount, with a particular emphasis on addressing the human factor. Future research should focus on innovative pedagogical approaches that not only impart technical knowledge but also foster a culture of security consciousness. This may involve gamification, virtual reality simulations, or adaptive learning systems that can tailor training to individual needs and learning styles.

The arena of international cooperation in cybersecurity calls for new models that can transcend current limitations. Researchers must explore innovative frameworks that can overcome challenges related to trust, sovereignty, and information sharing. This may involve the development of blockchain-based systems for

secure information exchange, the creation of international cyber peacekeeping forces, or the establishment of global cyber norms and treaties that can adapt to the rapid pace of technological change.

As cybersecurity measures become increasingly pervasive, their long-term societal impacts warrant scrutiny. Research into the psychological, social, and ethical implications of ubiquitous security measures is essential. This includes examining how constant surveillance and security protocols affect individual privacy, social trust, and democratic values. Understanding these broader impacts will be crucial in designing cybersecurity strategies that protect not only our digital assets but also our societal fabric.

The integration of AI in cybersecurity brings both promise and peril, necessitating the development of robust ethical frameworks. Future research should focus on creating guidelines that address issues of bias, transparency, and accountability in AI-driven security systems. This includes exploring methods for explainable AI in cybersecurity, developing fairness metrics for automated threat detection systems, and creating governance models that ensure the responsible use of AI in this critical domain.

Finally, the development of adaptive and resilient cybersecurity architectures represents a frontier of immense potential. Future research should focus on creating security systems that can evolve dynamically in response to emerging threats and changing technological landscapes. This may involve the exploration of bio-inspired security models, self-healing networks, or AI-driven systems that can anticipate and neutralize threats before they materialize.

Concluding Thoughts: Weaving the Web of Cyber Resilience

As we conclude this expansive exploration, we recognize that cybersecurity is not a destination but an ongoing odyssey—a process of continuous adaptation, learning, and evolution. Our theoretical framework offers a multifaceted lens through which we can view this journey, reminding us that effective cybersecurity requires a delicate balance of technology, human factors, ethics, and global collaboration.

In a world where data flows like digital rivers and information stands as the new gold, our approach to cybersecurity must be as dynamic and adaptable as the threats we face. By embracing a holistic perspective, we can weave a web of cyber resilience—one that is robust enough to withstand the tempests of current threats yet flexible enough to adapt to the winds of future challenges.

As we venture into the future, let these insights serve as a beacon, illuminating our path through the shadowy and complex realm of cybersecurity. In this vast digital ecosystem, each of us plays a vital role, entrusted with safeguarding not just data and systems but the very foundations of our interconnected global society.

The road ahead is undoubtedly fraught with challenges, but it also brims with opportunities for innovation, collaboration, and growth. By embracing a comprehensive, ethical, and cooperative approach to cybersecurity, we can collectively forge a more secure, resilient, and trustworthy digital future—a legacy of protection and empowerment for generations to come. In this ongoing narrative of technological progress and security challenges, we are not mere spectators but active authors, each contributing a crucial verse to the epic of our shared digital destiny.

APPENDIXES

Appendix A: Glossary of Key Cybersecurity Terms

1. **Advanced Persistent Threat (APT):** A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.
2. **Cyber Threat Intelligence (CTI):** Information that provides insights into cyber threats and risks to help organizations protect their assets.
3. **Distributed Denial of Service (DDoS):** An attack where multiple compromised systems are used to target a single system, causing a denial of service.

4. **Encryption:** The process of encoding information in such a way that only authorized parties can access it.
5. **Firewall:** A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
6. **Malware:** Software designed to disrupt, damage, or gain unauthorized access to a computer system.
7. **Phishing:** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website.
8. **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
9. **Social Engineering:** The psychological manipulation of people into performing actions or divulging confidential information.
10. **Zero-Day Exploit:** An attack that exploits a previously unknown vulnerability in a computer application or operating system.

Appendix B: Timeline of Major Cyber Attacks (2010-2024)

- **2010:** Stuxnet worm targets Iranian nuclear facilities
- **2013:** Target data breach affects 41 million consumers
- **2014**: Sony Pictures hack exposes confidential data
- **2015:** Ukraine power grid cyberattack causes widespread outages
- **2016:** DNC email leak impacts U.S. presidential election
- **2017:** WannaCry ransomware attack affects organizations worldwide
- **2018:** Marriott International data breach exposes 500 million guest records
- **2020:** SolarWinds supply chain attack compromises numerous organizations and government agencies
- **2021:** Colonial Pipeline ransomware attack disrupts fuel supply in the U.S.
- **2023:** MOVEit file transfer tool vulnerability exploited, affecting numerous organizations globally

Appendix C:

Tab.1: *Cybersecurity Frameworks Comparison*

Framework	Focus	Key Components	Best Suited For
NIST Cybersecurity Framework	Comprehensive cybersecurity approach	Identify, Protect, Detect, Respond, Recover	Organizations of all sizes and sectors
ISO/IEC 27001	Information security management	Risk assessment, security controls, continual improvement	Organizations seeking international certification
MITRE ATT&CK	Tactics and techniques used by adversaries	12 tactics, numerous techniques, and sub-techniques	Threat modeling and security operations
Cybersecurity Capability Maturity Model (C2M2)	Cybersecurity program maturity	10 domains, 4 maturity indicator levels	Energy sector organizations

Tab. 2: *Key Components of Cybersecurity Theoretical Framework*

Theory/Model	Key Concepts	Application to Cybersecurity
Socio-Technical Systems Theory	Integration of social and technical aspects	Emphasizes the need for a holistic approach considering technology, people, processes, and organizational factors
Protection Motivation Theory	Threat appraisal, coping appraisal	Explains individual security behaviors based on perceived threat severity, vulnerability, response efficacy, and self-efficacy
NIST Cybersecurity Framework	Identify, Protect, Detect, Respond, Recover	Provides a risk-based approach to managing cybersecurity risk
Cybersecurity Capability Maturity Model (C2M2)	Maturity levels, domain-specific practices	Assesses and improves cybersecurity capabilities, particularly in critical infrastructure sectors
Ethical Framework for Cybersecurity	Privacy, autonomy, fairness	Addresses ethical implications of cybersecurity measures
Human-Centric Security Model	Human as security asset, behavior transformation	Shifts perspective from humans as “weakest link” to potential “security heroes”
International Cooperation Model	Cross-border collaboration, information sharing	Addresses the global nature of cyber threats and need for international cooperation
Theory of Planned Behavior	Attitudes, subjective norms, perceived behavioral control	Explains factors influencing individuals' intentions to comply with security policies

Tab. 3: *Emerging Trends in Threat Intelligence*

Trend	Description	Potential Impact
AI-powered threat detection	Use of machine learning algorithms to identify and respond to threats	Faster threat detection, reduced false positives, improved predictive capabilities
Automated threat intelligence sharing	Real-time sharing of threat data between organizations and sectors	Enhanced collective defense, quicker response to emerging threats
Dark web monitoring	Proactive scanning of dark web forums for threat indicators	Early warning of potential attacks, insight into attacker tactics
Behavioral analytics	Analysis of user and entity behavior to detect anomalies	Improved detection of insider threats and advanced persistent threats
Threat intelligence platforms (TIPs)	Centralized platforms for aggregating and analyzing threat data	Better integration of threat intelligence into security operations
IoT-specific threat intelligence	Focused intelligence gathering for Internet of Things devices	Improved security for rapidly expanding IoT ecosystems
Cloud-native threat intelligence	Tailored intelligence for cloud environments	Enhanced security for organizations adopting cloud technologies

Trend	Description	Potential Impact
Geopolitical threat intelligence	Analysis of cyber threats in the context of global political events	Better understanding of nation-state threats and cyber warfare tactics

Tab. 4: *Critical Infrastructure Protection Strategies*

Strategy	Description	Challenges	Examples
Network segmentation	Dividing network into subnetworks to improve security	Complexity in implementation, potential impact on operations	Separating IT and OT networks in industrial control systems
Regular vulnerability assessments	Systematic review of security weaknesses	Resource intensive, keeping pace with evolving threats	Annual penetration testing of power grid control systems
Redundancy and resilience	Building backup systems and fail-safe mechanisms	Cost, complexity in design and maintenance	Redundant communication systems for emergency services
Supply chain risk management	Assessing and mitigating risks from third-party suppliers	Limited visibility into supplier practices, global supply chains	Vetting of technology vendors for telecommunications infrastructure
Continuous monitoring	Real-time surveillance of network activities and anomalies	Data overload, false positives	24/7 monitoring of financial transaction systems
Incident response planning	Developing and practicing response procedures for cyber incidents	Keeping plans updated, coordinating across departments	Regular tabletop exercises for water treatment facility breaches
Physical security integration	Combining cyber and physical security measures	Coordination between IT and physical security teams	Biometric access controls for data centers
Workforce training and awareness	Educating employees about cybersecurity risks and best practices	Engaging employees, measuring effectiveness	Regular phishing simulations for healthcare staff

Tab. 5: *Human Factors in Cybersecurity*

Factor	Description	Implications for Cybersecurity
Risk perception	How individuals perceive and evaluate cyber risks	Influences adoption of security measures and compliance with policies
Security fatigue	Exhaustion and resignation regarding security practices	Can lead to lax security behaviors and non-compliance
Social influence	Impact of peer behavior on individual security practices	Can be leveraged to promote positive security culture
Cognitive biases	Systematic errors in thinking that affect decision-making	Can lead to underestimation of threats or overconfidence in security measures

Factor	Description	Implications for Cybersecurity
Security awareness	Knowledge and understanding of security risks and best practices	Critical for creating a human firewall against social engineering attacks
Usability of security tools	Ease of use and integration of security measures into workflows	Affects adoption and correct usage of security technologies
Motivation and incentives	Factors that drive individuals to engage in secure behaviors	Can be used to design effective security awareness and training programs
Cultural factors	Influence of organizational and national culture on security attitudes	Necessitates tailored approaches to security across different contexts

Tab. 6: *Ethical Considerations in Cybersecurity*

Ethical Issue	Description	Potential Solutions
Privacy vs. Security	Balancing need for monitoring with individual privacy rights	Transparent policies, data minimization, privacy-preserving technologies
Informed Consent	Ensuring users understand and agree to security measures	Clear communication, opt-in policies for data collection
Algorithmic Bias	Potential for AI-driven security systems to perpetuate biases	Regular audits of AI systems, diverse training data, human oversight
Vulnerability Disclosure	Balancing public safety with potential for exploit	Responsible disclosure policies, bug bounty programs
Surveillance Ethics	Ethical implications of mass surveillance for security	Legal frameworks, oversight mechanisms, transparency reports
Cyber Warfare	Ethical considerations in offensive cyber operations	International agreements, rules of engagement for cyberspace
Digital Divide	Ensuring equitable access to cybersecurity measures	Capacity building initiatives, affordable security solutions
Dual-Use Technologies	Managing technologies that can be used for both protection and attack	Export controls, ethical guidelines for research and development

Tab. 7: *International Cybersecurity Cooperation Initiatives*

Initiative	Participating Entities	Key Objectives	Challenges
Budapest Convention on Cybercrime	65+ countries	Harmonize cybercrime laws, improve international cooperation	Limited participation from some major countries
UN Group of Governmental Experts (UN GGE)	UN member states	Develop norms for responsible state behavior in cyberspace	Competing national interests, lack of enforcement mechanisms
Paris Call for Trust and Security in Cyberspace	80+ countries, 700+ entities	Promote nine principles for securing cyberspace	Non-binding nature, implementation challenges

Initiative	Participating Entities	Key Objectives	Challenges
Global Forum on Cyber Expertise (GFCE)	90+ members	Strengthen cyber capacity building and expertise	Coordinating diverse stakeholders, measuring impact
INTERPOL Global Cybercrime Expert Group	Law enforcement agencies	Enhance international cooperation in cybercrime investigations	Jurisdictional issues, varying legal frameworks
NATO Cooperative Cyber Defence Centre of Excellence	NATO member and partner countries	Enhance cyber defense capabilities through research, training, and exercises	Balancing national sovereignty with collective defense
EU Network and Information Security (NIS) Directive	EU member states	Improve cybersecurity capabilities and cooperation within the EU	Harmonizing implementation across diverse national contexts
ASEAN-Japan Cybersecurity Capacity Building Centre	ASEAN countries, Japan	Develop cybersecurity capacity in the ASEAN region	Addressing varying levels of cyber maturity among members

REFERENCES

Aloul, F. A. (2012). The need for effective information security awareness. Journal of Advances in Information Technology, 1(4), 176-183. https://doi.org/10.4304/jait.1.4.176-183

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society, 11(3), 1-11.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004

Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 9, 220b-220b. https://doi.org/10.1109/HICSS.2006.110

Council of Europe. (2001). Convention on Cybercrime. European Treaty Series, 185. https://rm.coe.int/1680081561

Council of Europe. (2001). Convention on Cybercrime. European Treaty Series, 185. https://rm.coe.int/1680081561

Cyber Threat Alliance. (2017). Cyber Threat Alliance expands mission through appointment of President, formal incorporation as not-for-profit and launch of new threat intelligence sharing platform. https://cyberthreatalliance.org/cyber-threat-alliance-expands-mission-appointment-president-formal-incorporation-not-profit-launch-new-threat-intelligence-sharing-platform/

Cybersixgill. (n.d.). Threat intelligence solutions. https://www.cybersixgill.com/solutions/

Denning, D. E. (2012). Stuxnet: What has changed? Future Internet, 4(3), 672-687. https://doi.org/10.3390/fi4030672

French Ministry for Europe and Foreign Affairs. (2018). Paris Call for Trust and Security in Cyberspace. https://pariscall.international/en/

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, 2009(2), 5-10. https://doi.org/10.1016/S1361-3723(09)70019-9

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. 2014 47th Hawaii International Conference on System Sciences, 2025-2034. https://doi.org/10.1109/HICSS.2014.256

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics: An introduction (2nd ed.). Routledge.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal, 24(3), 1-8. https://doi.org/10.4018/irmj.2011070101

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. IT Professional, 19(5), 20-26. https://doi.org/10.1109/MITP.2017.3680959

Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, L. J. (2015). Towards a human factors ontology for cyber security. STIDS, 26-33.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. Journal of Homeland Security and Emergency Management, 11(4), 489-510. https://doi.org/10.1515/jhsem-2014-0035

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

SANS Security Insights, SANS Institute, & Petersen, M. (2020). 2020 SANS Cyber Threat Intelligence (CTI) Survey. https://www.sans.org/reading-room/whitepapers/analyst/2020-cyber-threat-intelligence-cti-survey-39395

Schneier, B. (2000). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296-298. https://doi.org/10.1038/d41586-018-04602-6

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. Computers & Security, 79, 68-79. https://doi.org/10.1016/j.cose.2018.07.012

U.S. Department of Energy. (2014). Cybersecurity Capability Maturity Model (C2M2). https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Energy. (2014). Cybersecurity Capability Maturity Model (C2M2). https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Homeland Security. (2016). National Cyber Incident Response Plan. https://www.us-cert.