ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

The Role of Cyberattacks on Modern Warfare: A Review

Dennis Redeemer Korda[1], Emmanuel Oteng Dapaah[2]

[1]*Department of ICT, Bolgatanga Technical University*

[2]*Department of ICT, E.P College of Education, Bimbilla*

DOI: https://doi.org/10.51584/IJRIAS.2023.8733

Received: 28 July 2023; Accepted: 02 August 2023; Published: 30 August 2023

Abstract: The role of cyberattacks in modern warfare has become increasingly important in recent years. Cyberattacks can be used to gain a tactical advantage over an adversary, disrupt or disable critical infrastructure, gather intelligence, as well as engage in offensive or defensive operations. They can also be used as part of psychological warfare to create a sense of fear and uncertainty among an adversary's population. As a result, military forces around the world are investing in cybersecurity and cyber warfare capabilities to prepare for the evolving threat landscape. This abstract highlights the growing importance of cyberattacks in modern warfare and the need for continued focus on developing and improving cybersecurity and cyber warfare capabilities.

Keywords: Cyberattacks, cybersecurity, Cyberwar, DDoS, Cyberspace,

I. Introduction

The past few years have seen a surge in cyberattacks. Cyberattacks are fragment of modern warfare. In Russia's war against Ukraine, they are being used to discourage and spread misinformation which could also have an unswerving influence on the combat zone. The very same day that Russian groups invaded Ukrainian territory, vital Kyiv government websites were suddenly unavailable together with that of the parliament, government, Foreign Ministry and other state institutions(*Russia-Ukraine Conflict: What Role Do Cyberattacks Play? | Europe | News and Current Affairs from around the Continent | DW | 28.02.2022*, n.d.).

Some of the hackers use distributed denial-of-service attack, known as DDoS, A DDoS attack involves multiple connected online devices, jointly identified as a botnet, which are used to overwhelm a targeted server, service or network with fake traffic. Data-wiper malware was first boomed in an operation in 2017 where a Russian wiper malware targeted Ukraine with the self-styled NotPetya malware that caused enormous economic damage (Milmo, 2022). This software was first detected on Ukraine computers and can destroy massive amounts of data. The cyberattack echoed a similar operation in 2017, when Russian wiper malware targeted Ukraine with the so-called NotPetya malware that caused enormous economic damage. These two forms of attacks are not really enough to the change the outcome of the war in Ukraine, however, it crystal clear that these attacks are not only targeting critical Information Technology infrastructure but there are also ruminants of false information. All these attacks occur in the cyberspace and since these attacks target primarily data, it is imperative to take the necessary steps to protect data(Hodowu et al., 2020; Korda et al., 2021).

II. Literature Review

Modern warfare has increasingly incorporated cyberattacks as a crucial part of its operations. These attacks can be used for espionage, disruption, and destruction of enemy targets, and can cause significant harm to critical infrastructure and military operations. This literature review provides an overview of the research on the role of cyberattacks in modern warfare, with a focus on the types of attacks, their impact, and the strategies used to prevent and detect them.

Cyberattacks in modern warfare can take many forms, including phishing, ransomware, malware, and denial-of-service attacks (DoS). A study by (Ferrara & Zhou, 2019) found that state-sponsored cyberattacks are becoming more sophisticated and using multiple methods to achieve their objectives. These attacks can be used to disrupt critical infrastructure, gain access to sensitive information, or cause physical damage to military operations.

The impact of cyberattacks on modern warfare can be significant, causing disruption to critical infrastructure, compromising sensitive information, and even causing physical harm to military personnel. A study by (Denning, 2016) found that cyberattacks can be used to undermine the confidence of military personnel in their own systems, leading to operational inefficiencies and reduced effectiveness in combat.

Preventing and detecting cyberattacks in modern warfare requires a multi-faceted approach that includes technical, organizational, and policy measures. A study by (Duggan, Rafique, & Callaghan, 2019) found that network segmentation, multi-factor authentication, and regular vulnerability scanning are effective measures for preventing and detecting cyberattacks. Continuous monitoring and threat intelligence can also be used to detect and respond to cyberattacks in real time (Stewart, 2017).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

Cyberattacks have become an increasingly important part of modern warfare, with state-sponsored attacks becoming more sophisticated and difficult to detect. The impact of these attacks can be significant, causing disruption to critical infrastructure, compromising sensitive information, and even causing physical harm to military personnel. Effective prevention and detection strategies are essential to minimizing the impact of cyberattacks on military operations. Technical, organizational, and policy measures, including network segmentation, multi-factor authentication, regular vulnerability scanning, and continuous monitoring and threat intelligence, can all be used to prevent and detect cyberattacks in modern warfare.

III. Ultimate Concepts

Cyberattacks play an increasingly important role in modern warfare, as they can be used to gain a tactical advantage over an adversary, disrupt or disable critical infrastructure, and gather intelligence. Here are some of the ways in which cyberattacks can impact modern warfare:

Sabotage and Disruption: Cyberattacks can be used to sabotage or disrupt an adversary's military capabilities, including critical infrastructure such as power grids, transportation systems, and communication networks. This can cause confusion, chaos, and uncertainty on the battlefield, and can help to give the attacker an advantage.

Intelligence Gathering: Cyberattacks can be used to gather intelligence on an adversary's military capabilities, including troop movements, weapon systems, and communication networks. This information can be used to plan attacks or to defend against enemy actions.

Offensive Operations: Cyberattacks can be used as part of offensive operations, such as disabling an enemy's command and control systems, disrupting logistics operations, or interfering with the enemy's ability to communicate.

Defense: Cyberattacks can also be used as part of defensive operations, such as detecting and blocking incoming attacks, monitoring network traffic for signs of intrusion, and hardening critical infrastructure against cyber threats.

Psychological Warfare: Cyberattacks can also be used to create a sense of fear, uncertainty, and doubt among an adversary's civilian population or military personnel. This can undermine the enemy's morale and create divisions within their ranks, ultimately weakening their ability to fight.

Overall, cyberattacks have become an important part of modern warfare, and their impact on military operations is likely to continue to grow in the future. As a result, military forces around the world are increasingly investing in cybersecurity and cyber warfare capabilities to prepare for the evolving threat landscape.

Specifically, as at September 2021, there were several types of cyberattacks that were reported to be used in the ongoing conflict between Russia and Ukraine. These include:

Phishing attacks: Russian hackers were reported to have used phishing attacks to gain access to Ukrainian government and military networks. These attacks typically involve sending fraudulent emails that appear to be from a trusted source, in order to trick the recipient into revealing sensitive information or downloading malware.

Malware attacks: Malware, including ransomware, has been used to target Ukrainian organizations and critical infrastructure, such as the country's energy sector. These attacks can be used to disrupt or disable systems, or to steal sensitive information.

Distributed Denial of Service (DDoS) attacks: DDoS attacks involve flooding a website or network with traffic in order to overwhelm it and make it unavailable to users. Ukrainian government and military websites have been targeted with DDoS attacks, which can be used as a means of disrupting communications and operations.

Supply chain attacks: Russian hackers have been known to target third-party software vendors and suppliers that are used by Ukrainian organizations, in order to gain access to their networks. This type of attack can be particularly effective, as it can give the attacker access to a large number of organizations and networks through a single point of entry.

It is important to note that the types of cyberattacks used in the Russian-Ukrainian conflict may evolve and change over time, as both sides continue to develop new tactics and techniques.

IV. Modes of Execution and Prevention

Phishing Attacks:

Phishing attacks are a common tactic used by hackers to gain unauthorized access to sensitive information or networks. In the context of the Russian-Ukrainian conflict, Russian hackers have been known to use phishing attacks to target Ukrainian government and military personnel. These attacks typically involve sending fraudulent emails that appear to be from a trusted source, such as a colleague or a superior officer, in order to trick the recipient into revealing sensitive information or downloading malware. In 2022,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

the quantity of phishing attacks surged by 100% and exceeded 500 million. Kaspersky's anti-phishing system was able to block over 500 million fraudulent website access attempts in 2022, which is twice as much as the number from 2021 (Kaspersky, 2023).

How they are launched: Phishing attacks are often launched through email or instant messaging. The attacker will typically create a fake email address or account that appears to be from a trusted source. The email will contain a message designed to lure the recipient into taking a specific action, such as clicking on a link, downloading an attachment, or entering login credentials into a fake login page. Once the recipient takes the desired action, the attacker gains access to their network or sensitive information. The diagram below illustrates how these attacks are carried out.

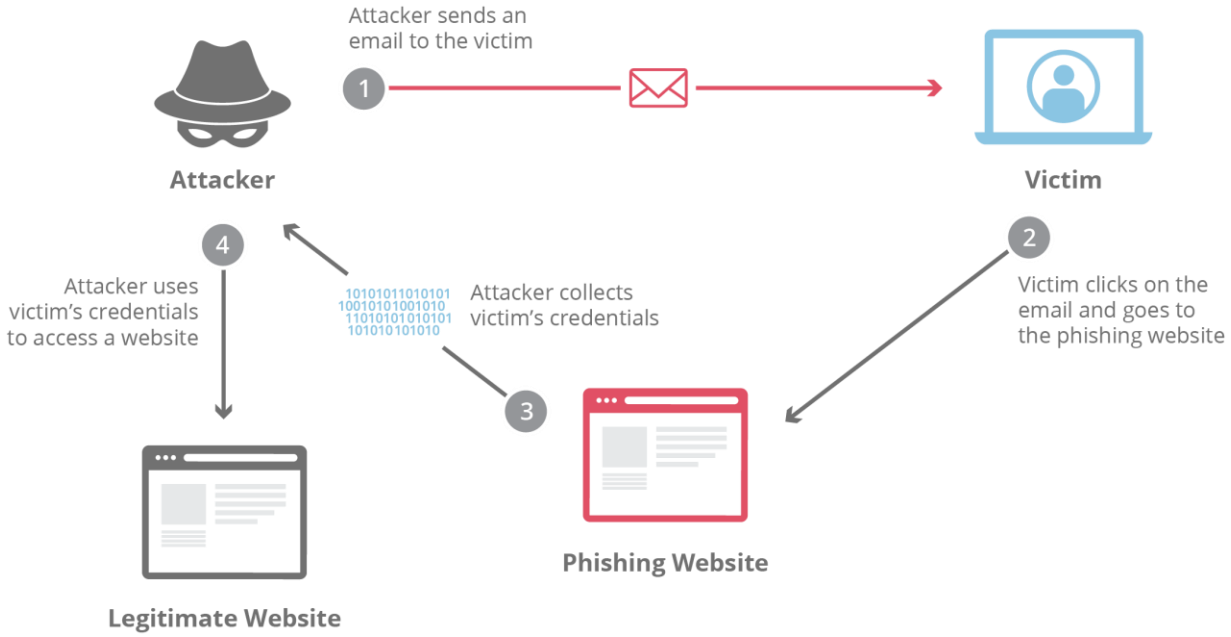

Fig. 1 Phishing attack process

Prevention

To prevent phishing attacks, organizations can take several steps, including:

- Security awareness; Educating employees on how to recognize and avoid phishing emails.
- Enforcing strong password policies.
- Implementing multi-factor authentication, which requires users to provide multiple forms of identification before accessing sensitive information
- Using spam filters and other email security measures to identify and block phishing emails before they reach employees' inboxes

Malware Attacks:

Malware attacks involve the use of malicious software, such as viruses, worms, and trojans, to gain unauthorized access to a network or system. In the context of the Russian-Ukrainian conflict, malware has been used to target Ukrainian organizations and critical infrastructure, such as the country's energy sector.

How they are launched: Malware attacks can be launched through a variety of methods, including phishing emails, drive-by downloads from compromised websites, and infected software or hardware. Once the malware is installed on a system, it can be used to steal sensitive information, disrupt operations, or gain unauthorized access to other systems.

Prevention

To prevent malware attacks, organizations can take several steps, including:

- Keeping software and operating systems up to date with the latest security patches

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

- Using antivirus software and other security measures to detect and remove malware
- Limiting the use of administrator privileges, which can be used to install malware or make unauthorized changes to a system
- Implementing network segmentation and other access control measures to limit the impact of malware if it does infect a system

Distributed Denial of Service (DDoS) Attacks:

DDoS attacks involve flooding a website or network with traffic in order to overwhelm it and make it unavailable to users. In the context of the Russian-Ukrainian conflict, DDoS attacks have been used to target Ukrainian government and military websites.

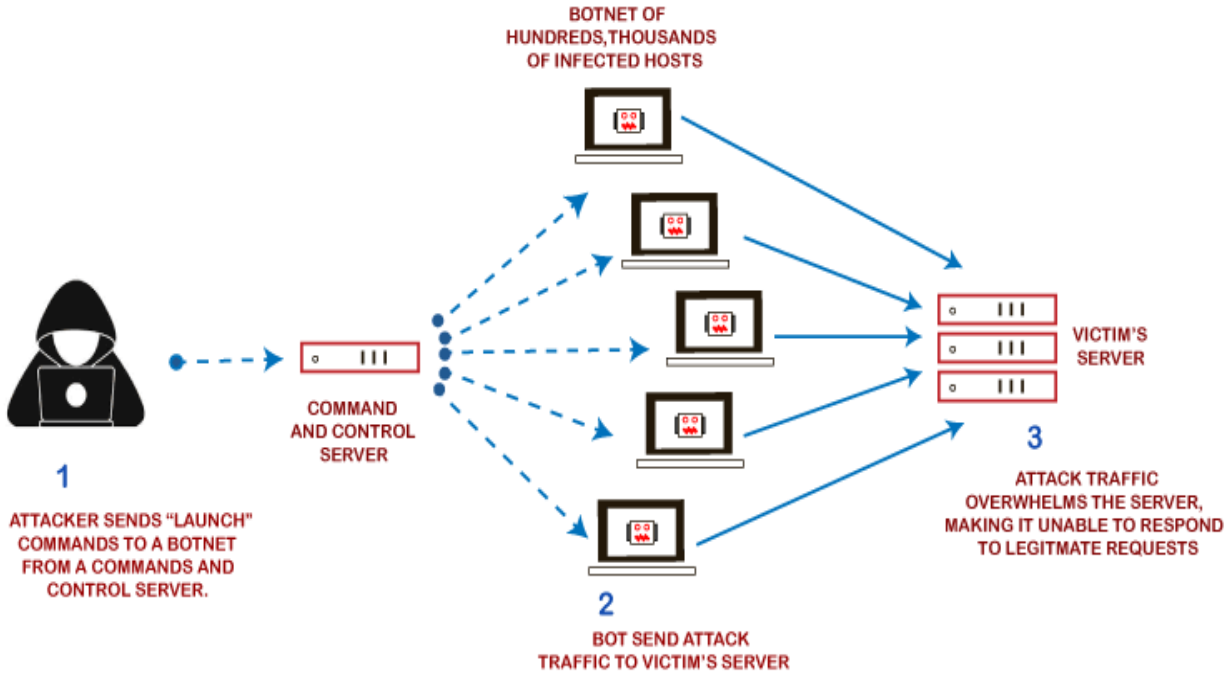

Fig. 2 DDoS attack process

How they are launched: DDoS attacks are typically launched using a botnet, which is a network of compromised devices that can be controlled remotely. The attacker will send a large volume of traffic to the target website or network, using the botnet to amplify the attack and make it more difficult to defend against.

Prevention

To prevent DDoS attacks, organizations can take several steps, including:

- Implementing web application firewalls and other network security measures to detect and block DDoS traffic
- Using content delivery networks (CDNs) to distribute traffic across multiple servers, which can help to absorb DDoS attacks
- Working with Internet Service Providers (ISPs) to block traffic from known botnet sources
- Implementing rate limiting and other traffic management measures to prevent DDoS attacks

V. Cybersecurity Policies and Procedures

Cybersecurity policies and procedures are essential for detecting and preventing cyberattacks in modern warfare. With the increasing dependence on technology in military operations, it has become essential to establish effective cybersecurity protocols to protect critical infrastructure and sensitive information. This report will outline some essential cybersecurity policies and procedures that can be implemented to detect and prevent cyberattacks on modern warfare.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

Implement Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is an essential security measure that requires users to provide two or more forms of authentication before accessing a system or application. MFA can help prevent unauthorized access and enhance security by making it more difficult for attackers to gain access to sensitive information.

MFA requires users to provide at least two forms of authentication before accessing a system or application. Typically, MFA requires a combination of something the user knows (such as a password or PIN) and something the user has (such as a smart card or mobile device) or something the user is (such as biometric data like fingerprints or facial recognition).

MFA helps prevent cyberattacks in several ways. Firstly, it makes it much more difficult for attackers to gain unauthorized access to sensitive information. If an attacker obtains a user's password through a phishing attack or other means, they will not be able to gain access to the system without also having the additional form of authentication. This reduces the risk of a successful cyberattack. Secondly, MFA can also help detect potential cyberattacks. If an attacker attempts to log in to a system using a user's credentials, MFA may trigger an alert or block the login attempt, as the attacker is unlikely to have access to the additional form of authentication. This can alert security teams to potential unauthorized access attempts and allow them to take appropriate action.

Overall, MFA is an essential security measure that can help detect and prevent cyberattacks by adding an extra layer of protection to the login process. By requiring multiple forms of authentication, MFA reduces the risk of successful cyberattacks and provides additional visibility into potential security incidents. MFA should be implemented across all systems and applications that hold sensitive information.

Network Segmentation

Network segmentation is another essential cybersecurity technique that can help detect and prevent cyberattacks. By separating networks into different segments, organizations can limit the impact of cyberattacks and prevent them from spreading to other parts of the network. This can also help with network monitoring and incident response, as it allows for more targeted and effective detection and mitigation of cyber threats.

By creating different zones or segments within a network, organizations can limit the attack surface, control traffic flow, and better protect critical assets. Network segmentation can detect and prevent cyberattacks in several ways:

Limiting the impact of cyberattacks: If a cyberattacker is able to gain unauthorized access to a network segment, network segmentation can limit the impact of the attack by preventing the attacker from moving laterally to other parts of the network. By restricting access between network segments, an organization can contain an attack to a single segment, minimizing the impact of the attack and reducing the risk of data loss or system compromise.

Reducing the risk of insider threats: Network segmentation can also reduce the risk of insider threats by restricting access to sensitive information and resources. By limiting access to only those users who need it, an organization can reduce the risk of insider threats, such as data theft or sabotage.

Enhancing network monitoring: Network segmentation can also help with network monitoring and incident response. By creating smaller segments, an organization can more easily monitor network traffic, identify potential anomalies or suspicious activity, and respond quickly to potential security incidents.

Control traffic flow: By segmenting the network, you can control the flow of traffic between segments. This can allow you to prevent certain types of traffic from moving between segments, such as peer-to-peer file sharing or other high-risk activities.

Network segmentation is an essential security measure that can help detect and prevent cyberattacks by limiting the attack surface, containing the impact of potential attacks, reducing the risk of insider threats, enhancing network monitoring, and controlling traffic flow.

Regular Vulnerability Scanning

Regular vulnerability scanning is critical to identifying and addressing potential vulnerabilities in a network or system. These scans should be performed regularly, and the results should be analyzed to determine which vulnerabilities require immediate attention. Vulnerability scanning can be performed using automated tools, which can save time and resources, and should be conducted across all systems and applications.

Vulnerability scanning involves using automated tools to search for known vulnerabilities in a network, system, or application and generating reports on potential weaknesses. Regular vulnerability scanning can detect and prevent cyberattacks in several ways:

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

Identifying security weaknesses: Vulnerability scanning can identify security weaknesses in an organization's IT systems and applications before cyberattackers can exploit them. By regularly scanning for vulnerabilities, an organization can stay on top of potential security threats and take action to patch or mitigate vulnerabilities before they can be exploited.

Prioritizing remediation efforts: Vulnerability scanning can also help prioritize remediation efforts by providing a risk-based assessment of vulnerabilities. The scanning tool can assign a risk score to each vulnerability, allowing an organization to prioritize which vulnerabilities to address first based on the level of risk they pose.

Compliance requirements: Vulnerability scanning is often a requirement for compliance with industry regulations or standards. By regularly scanning for vulnerabilities, an organization can demonstrate compliance with security requirements and avoid potential penalties or fines.

Ongoing monitoring: Regular vulnerability scanning can also be used for ongoing monitoring of an organization's IT systems and applications. By scanning for vulnerabilities on a regular basis, an organization can ensure that new vulnerabilities are identified and addressed as soon as possible.

Regular vulnerability scanning is an important security measure that can help detect and prevent cyberattacks by identifying vulnerabilities in an organization's IT systems and applications. By prioritizing remediation efforts, demonstrating compliance with security requirements, and providing ongoing monitoring, vulnerability scanning can help reduce the risk of successful cyberattacks.

Continuous Monitoring and Threat Intelligence

Continuous monitoring and threat intelligence are essential cybersecurity practice that help to detect and prevent cyberattacks. By monitoring network traffic, system logs, and other data, organizations can identify anomalies and potential threats in real-time, allowing for more effective threat detection and response. Threat intelligence, such as information about known threats and attack patterns, can also be used to proactively defend against cyberattacks.

Continuous monitoring involves the ongoing collection and analysis of data from an organization's IT systems, applications, and network, while threat intelligence involves the collection and analysis of data on potential security threats and vulnerabilities. Continuous monitoring and threat intelligence can detect and prevent cyberattacks in several ways:

Real-time threat detection: By continuously monitoring an organization's IT systems and network, security teams can quickly detect potential security threats or suspicious activity. Threat intelligence can also help identify emerging threats or vulnerabilities that may not yet be widely known, allowing organizations to proactively protect against them.

Incident response: Continuous monitoring and threat intelligence can also help with incident response by providing real-time information on potential security incidents. By quickly identifying potential threats, organizations can take immediate action to contain the incident and prevent further damage.

Enhanced threat intelligence: By combining continuous monitoring and threat intelligence, organizations can gain a more comprehensive understanding of potential security threats and vulnerabilities. By analyzing data from multiple sources, including internal systems and external threat intelligence feeds, organizations can gain insights into emerging threats and vulnerabilities, and take proactive steps to protect against them.

Improved security posture: Continuous monitoring and threat intelligence can also help organizations improve their overall security posture by providing ongoing insights into potential vulnerabilities and weaknesses. By continuously monitoring and analyzing data, organizations can identify and address potential security gaps, and take steps to improve their overall security posture.

Continuous monitoring and threat intelligence are essential security measures that can help detect and prevent cyberattacks in real-time. By providing real-time threat detection, incident response, enhanced threat intelligence, and improved security posture, these measures can help organizations stay ahead of potential security threats and vulnerabilities, and better protect their critical assets.

Regular Employee Training and Awareness

Regular employee training and awareness is a critical component of any cybersecurity policy. Employees should be trained on the importance of cybersecurity, best practices for password management, and how to identify potential threats, such as phishing emails or suspicious network activity. Regular training can help reduce the risk of human error, which is a common cause of cybersecurity incidents.

Effective cybersecurity policies and procedures are critical to detecting and preventing cyberattacks in modern warfare. Multi-factor authentication, network segmentation, regular vulnerability scanning, continuous monitoring and threat intelligence, and regular employee training and awareness are all essential components of an effective cybersecurity strategy. By implementing these policies and procedures, organizations can reduce the risk of cyberattacks and better protect critical infrastructure and sensitive information.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS | Volume VIII Issue VII July 2023

VI. Conclusions

In conclusion, the role of cyberattacks in modern warfare cannot be overstated. With the increasing reliance on digital infrastructure and technology in military operations, the impact of cyberattacks can be significant, ranging from disruption of critical infrastructure to intelligence gathering and offensive or defensive operations. As such, it is crucial for military forces around the world to continue to develop and improve their cybersecurity and cyber warfare capabilities to defend against these evolving threats. The ability to detect and respond to cyberattacks will be a critical component of modern warfare in the years to come, and those who are able to effectively incorporate cyber capabilities into their strategies will have a significant advantage on the battlefield.

References

1. Denning, D. E. (2016). The ethics of cyberwarfare. In The Ethics of Information Warfare. Springer, 31-50.
2. Duggan, M. J., Rafique, A., & Callaghan, V. (2019). A survey of cybersecurity policies and procedures in modern military operations. IEEE Access, 153492-153501.
3. Ferrara, E., & Zhou, B. (2019). State-sponsored cyberattacks in modern warfare. Cybersecurity Handbook, 269-285.
4. Hodowu, D. K., Korda, D. R., & Ansong, E. (2020). An Enhancement of Data Security in Cloud Computing with an Implementation of a Two-Level Cryptographic Technique, using AES and ECC Algorithm. International Journal of Engineering Research & Technology, 09(09).
5. Kaspersky. (2023, February 16). Kaspersky. Retrieved from Corporate News: https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022
6. Korda, D. R., Ansong, E., & Hodowu, D. K. (2021). Securing Data in the Cloud using the SDC Algorithm. International Journal of Computer Applications, 183(25), 24-29.
7. Milmo, D. (2022, February 24). The Guardian. Retrieved from Russia Unleased Data-Wiper Malware on Ukraine, says Cyber experts: https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts
8. Stewart, B. (2017). Continuous monitoring and threat intelligence in the 21st century. Advanced Persistent Security, 59-78.