ISSN (Print) XXXX-XXXX
ISSN (Online) XXXX-XXXX

Advanced Research Journal of Computer Science
Received: August 20, 2025 | Accepted: November 21, 2025 | Published: December 29, 2025
Volume 01, Issue 01, Pages 23-29
DOI https://doi.org/10.XXXXX/arjcs.2025.01.01.04

OPEN ACCESS
Check for updates

Cyber Warfare Strategies: An Examination of Various Approaches

Sinan Antoon[1*]
[1]University of Babylon, College of Medicine, Iraq

Author Designation: [1]Researcher

*Corresponding author: Sinan Antoon.

How to Cite the Article:
Antoon, Sinan. "Cyber Warfare Strategies: An Examination of Various Approaches." Advanced Research Journal of Computer Science, vol. 01, no. 01, 2025, pp. 23-29.

Abstract | Recently, the scope of cyber warfare has expanded dramatically, with attacks becoming more frequent and sophisticated. This form of confrontation differs from traditional twentieth-century military conflicts like the First and Second World Wars, as it uses modern technology to strike at nations, governments, and military systems. Although "war" usually implies physical combat, cyber warfare often causes disruption without direct loss of life, while still generating serious political, economic, and security repercussions. The United States has placed considerable emphasis on cyber operations, using these strategies to collect vital intelligence on adversaries and help reduce the risks of terrorism. This warfare style is applied across many scenarios, particularly when military entities seek early warning regarding potential attacks, strategic plans, or enemy weapon deployment. Such information is gathered through digital intrusion, monitoring, and sophisticated cyber tools. Furthermore, cyber warfare has been effective in weakening hostile nuclear development programs. A notable case is the attack on Iranian nuclear facilities, where the Stuxnet worm was reportedly used to damage essential reactor functions. While no official group admitted responsibility, the involvement of US and Israeli military forces was widely believed. These developments stress the importance of nations investing in cyber capabilities and defenses to stop hostile acts and enhance national security. Cyber warfare is defined by its unique environments, actors, and technical methods, which shape the nature of today's digital conflicts.

Key Words Network Exploitation, Cyberwarfare, Cyber-Attacks and Cyber Exploitations

INTRODUCTION

Information technology has profoundly impacted how things are done in almost every industry. It's been dubbed "digital migration" because things have shifted from analog to modern systems. It is becoming increasingly common for businesses and other organizations to adapt their operations to the latest technology. The defense sector, for example, has invested heavily in information technology. In the modern era of warfare, things are pretty different from a few decades ago. Today's methods of conflict are vastly different from those of the First and Second World Wars. Some examples include planning, investigations and even the machines used. As a result, the term "cyber warfare" was coined. To put it simply, cyberwarfare is the use of cutting-edge technology to attack governments or countries. Weaponry can be used in this type of attack to cause as much damage as in actual warfare [1]. Contrary to popular belief, warfare in the digital age need not always imply physical violence. The term "cyber-warfare" does not have to mean violence or protracted conflict as is commonly associated with war. It's a form of competition that can be waged without resorting to violence, but the consequences will be enormous [2]. Many countries have tried cyber warfare in the recent past and while some have failed miserably, others have been spectacularly successful. The subject of cyberwarfare has recently gained a lot of traction. Armed forces, intelligence agencies and law enforcement agencies have prioritized computer security as a top investment and recruitment priority. The current push to gain a foothold in cyberspace is so intense that many governments will go too far, with disastrous consequences worldwide for democracy and human rights. The term "cyberwarfare" refers to computers and networks in military conflict. Cyberattacks, espionage and sabotage are just some of the threats that need to be considered.

There has been a discussion concerning whether or not these efforts may be classified as military action. Also included in alternative definitions of cyber warfare are non-state actors like terrorist organizations and companies and extremist political or ideological groups like hacktivists and transnational criminal organizations. A nation-intrusion states into another nation's computer systems, or networks can serve a variety of reasons, including causing harm or disruption.

The Target of Cyber-Attack

The majority of people believe that cyberattacks are not relevant to their lives. According to them, this is a problem for the state or the institutions involved in national security. This kind of thinking is a big problem when it comes to cybersecurity. Cyberattacks have to be kept under wraps until the very last minute. Before the real target is revealed, there must be sufficient time to ensure an effective strike. Even though hackers use a variety of weapons, they are still combatants in the same way that soldiers are. There are many similarities between this and conventional war. Therefore, we must be prepared to deal with the possibility of future conflicts that include attacks on a state's essential communication and information nodes [3-6]. It's only as safe as the weakest link in a network. A computer's connection to a computer network poses the most significant danger. Developing an information society presents a risk because it relies on information and communication technology. When a state's governance is highly informative, it is far more vulnerable than not. Because of this, cyberwar is a real threat to countries like the United States. We all have the opportunity to participate in it and we all have the chance to be victims of it. However, while modern technology makes our lives simpler, there is also a greater danger of being abused. Current states can be paralyzed much more quickly because they rely on digital processing and information exchange. As a result, the most advanced countries and their modern armies cannot ignore cyber security. An attack on technology control elements can have severe consequences for people's lives, businesses, or technology. Thus, a cyberattack can be defined as an attack on the infrastructure of information technology to damage or obtain sensitive or strategic information. Political and military motivations are the most common associations with this term. The threat of cyberattacks will soon outweigh the threat of terrorism.

Cyber-Warfare Tools and Techniques

A Cloud-Based System: Many security systems are undergoing significant transformations as a result of the cloud. Because many government organizations use cloud technology to store most of the sensitive data they produce regularly, this is the case. The military is an essential part of the government's administration, so it is included in discussions about the government. The cloud's critical information is constantly under attack and threat. The military has attempted to access or even alter data stored in the cloud on numerous occasions. Vulnerability emerges at this point. If you want to access or edit cloud data, you'll have to use the network system, introducing a new set of complications. Network-based system: - The utilization of interconnected systems for various reasons, such as communication, resource sharing and so on, is at the heart of networking technology. There are multiple ways to send information between offices or to various destinations. Military networking relies heavily on technology, which has evolved over the last few years. The military uses a wide range of communication methods, including satellites. Optic cables and wireless communication, for example. We have switches, routers, SDN architecture (software-defined networks), structured cabling and under-wired communications. Wireless LAN (WLAN), Wireless Access points, cloud-based control and on-premises control are all part of wireless networking. PTP Backhaul (point-to-point), Mesh Networks, PMPs and Wireless Encryption are also used in outdoor wireless networks.

Methods Used in Cyber Warfare

In recent years, as the number of internet users has increased, propaganda may now be spread more swiftly and effectively through cyberspace rather than through leaflet distribution. According to the Virus Bulletin, malware is becoming easier, more accessible and more rapid to propagate as the number of individuals who use the Internet continues to expand. Because of this, cyberattacks are more likely to occur in the future. Cyber-attacks can take a variety of forms, ranging from subtle to ruthless, as shown below:

Malware

Countries can conduct cyber-attacks against other countries by employing various viruses in their efforts. According to the definition, malware is any software that has been purposefully designed to cause harm to a computer system, computer network, or server. After the malware has been successfully implanted or placed into the victim's computer, it will begin to function as intended. They can take many different forms, including scripts, directly executable code and other types of programming. These destructive programs can perform various activities depending on the attacker's intentions. Cybercriminals are capable of altering data, stealing confidential information, encrypting or decrypting personal data, monitoring what users are doing and hijacking core computing functions of a computer without the permission of legitimate users or owners of the data [7]. These dangerous programs and files have been employed in the past for cyber warfare and some examples include computer viruses, Trojan horses, worms, ransomware, spyware, scareware and adware, among other things. As of 2020, the average ransomware payout was $111,605, a rise of 33% from the previous year. There were 10,573 harmful mobile applications blocked daily on average last year. Almost all malware is transmitted via email. Ransomware attacks on

enterprises cost an average of $133,000. One-half of all infected email attachments are Microsoft Office files. With 18.2% of all ransomware attacks, the United States has the highest percentage of ransomware detections. More than half of all bad domains are linked to spam campaigns. When they are first registered, most malicious domains are less than a week old [8].

Net Traveler Cyber-Attacks

This is a form of spyware that has been actively utilized since 2004 and is still being used today. It is a technique that has been programmed to infect high-profile servers with malicious software and data. This malware has been reported to have been deployed in several countries, with the victims claiming that their systems and servers have been hacked as a result. The malware was given this moniker because of how the attack was displayed on the user's computer. The name is derived from the previously used versions with the "Net Traveler is running!" It is mainly used by attackers that carry out advanced persistent threats to survey victims and it is particularly effective. They will be able to analyze all information that has been processed and all information that has been stored into the servers once they have been successfully installed into the system of the victims, after which the attacker will be able to transfer large volumes of this information to their desired destinations. Net Traveler technologies have been utilized to assault various high-profile targets in the past. Such marks are examples of nuclear power plants, government offices and embassies in multiple countries. Those participating in this attack employed over 100 URLs and were based in the United States, China and Hong Kong [9].

Espionage

This technique is derived from the common phrase "spy," which means "spyware." High-level technology is employed to spy on other countries' activities in this type of attack. This is pretty typical among superpower nations, which continually spy on one another to find out what they are up to, especially when it comes to weapons of mass destruction. Some have maintained that espionage is not a war crime. However, this is not always the case, as some instances of espionage can cause significant tensions between various nations, as has happened in the past. Espionage can be defined as the process through which an individual or a group of individuals obtains confidential or secret information or the act of disclosing the information without the owner's permission [10]. This is accomplished in the majority of cases through the employment of viruses. The "Titan Rain" probes of US defense computer systems contractors, for example, are an example of espionage that has been observed in the military over recent time. After realizing that there had been a series of attacks on their government systems, including the defense forces, the United States federal government established the Titan Rain. They eventually discovered that the attacks were being launched from the Chinese province of Guangdong. They were able to accomplish this by acquiring access to the computer networks of the majority of American defense contractors. Many cyberespionage campaigns have been linked to Advanced Persistent Threats (APTs), which are groups that have both the capability and intent to target a specific entity over an extended period. Nevertheless, APTs haven't restricted themselves to cyberespionage; they've also destroyed systems and data (sabotage) and disrupted business operations in other ways. The most common methods of cyberespionage have been uncovered. In addition to malware distribution, social engineering and spear phishing, these include watering hole attacks. There are many examples of malware that target government computers, such as Flame, which can switch on webcams and microphones, take screen photos of infected computers and transfer data and commands over Bluetooth, among other things. A government agency targeted a virus variant named Gauss, similar to Flame in its goals. Data about network connections, disks and system processes and folders were harvested by Gauss, which was meant to transmit this information to a server under the control of individuals who planted the malware. Cyberespionage frequently employs social engineering, in which the target is tricked into divulging information or performing another action by a perpetrator. Sophisticated cyberespionage attacks have used the method of "spear phishing," which is the practice of sending malicious attachments or links over email to trick the recipient into clicking on the wing or link. Since then, numerous reports have surfaced claiming that a spyware developer has made tools and capabilities available to various state actors from multiple nations to hack into devices via customized SMS and WhatsApp messages. In the past, intrusion software has been used to violate human rights and target journalists and activists, but export control regimes have been criticized as weak and problematic. Hacking tools that are publicly available online have made cyberespionage viable. Hacking tools such as zero-day exploits and implants are among the most commonly used methods of infiltrating systems and bypassing firewalls (e.g., backdoor, a secret portal used to gain unauthorized access to plans, or a Remote Access Tool or RAT). Shadow Brokers, a hacker collective, has released hacking tools since 2016. One of them is an EternalBlue exploit, part of the WannaCry ransomware that targeted and harmed healthcare, transportation and other worldwide systems (Figure 1).

Denial of Service (DOS) and Distributed Denial of Service (DDOS)

A technique used to make users' normal operations more difficult or even impossible to complete. A distributed Denial of Service (DDoS) attack targets a network, online resources, or military website to prevent legitimate users from accessing the network or system. The attackers will accomplish this by sending a continuous and quick request to a target server from a single device connected to a single internet connection. A timer is programmed to run continuously until the server's bandwidth is overburdened, at which point the process will be terminated. It operates so that the software vulnerability in the system will be exploited and as a result, the server's CPU or computer RAM will be continually depleted.

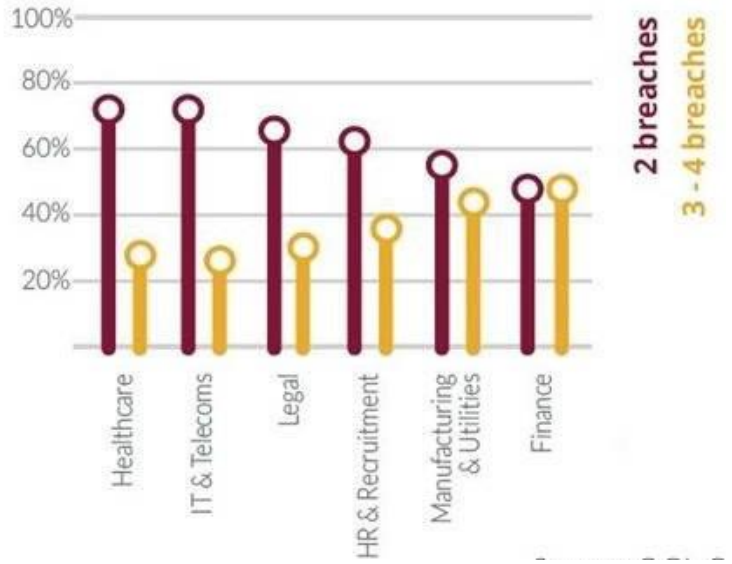

Figure 1: Industries are Most Vulnerable to Cyber-Attacks, Having Had More Than One Breach

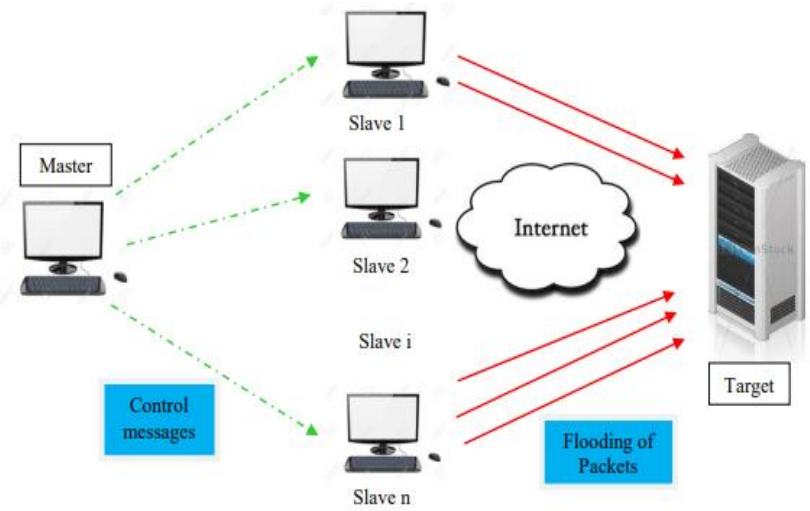

Figure 2: Distributed Denial of Service Attack

In the military, when time is significant and tasks must be completed within a specified time frame, delays in the system induced by Denial-of-Service (DoS) attacks can result in substantial damage. The following are some of the potential consequences of this technology: Network congestion, military mission failures and service interruptions are all examples of service interruptions.

The main DDoS attacker sends control messages to the enslaved people on the Internet, as shown schematically in Figure 2. Attack packets (in red) are sent to the target system by the enslaved people, unaware they are doing so. Several factors contribute to the prevalence of DDoS attacks today, including personal motives (such as vengeance) for which an attacker targets specific computers, prestige gains (such as gaining the respect of other hackers), monetary gains (such as blackmailing online businesses) and political motives (such as compromising an enemy's resources). Cybercrime damages in 2020 are estimated at roughly $400 billion and are predicted to rise to approximately $2 trillion in 2021 [11]. According to statistics, DDoS attacks accounted for 3.57% of all cyberattacks from January to September. Malware (35.61%), Vulnerability (6.41%), Targeted Attack (12.61%), Account Hijacking (17.33%) and Unknown Attacks all had more significant percentages than DDoS attacks (16.60%). There will be 15.4 million DDoS attacks in the world in 2023. IoT-related attacks increased threefold in the first half of this year. 2018 saw a 1,000-fold rise in the number of malicious PowerShell scripts prevented on the endpoint compared to 2017. The third most common IoT threat in 2018 was the Mirai-distributed DDoS worm. Internal actors are responsible for 30% of data breaches. An average of 5,200 attacks are made on IoT devices each month. Cryptocurrency mining is responsible for 90% of remote code execution threats. About 69% of firms say

their anti-virus software cannot block the dangers they are witnessing. High-risk apps are installed on one out of every thirty-six mobile devices.

Sabotage

The term "cyber-sabotage" refers to state and non-state entities attempting to disrupt a nation's computer networks and censorship infrastructure. The government must assess what information is classified as sensitive and what the consequences would be leaked. Insider threats, such as dissatisfied or negligent employees, or government staff affiliated with the attacking country, can be used by hostile countries or terrorists to steal or destroy information. A nation's critical infrastructure is frequently targeted by cyberattacks carried out by both state and non-state actors. It is possible to utilize sabotage for various purposes, from causing government services to be disrupted to extortion and surveillance demands by foreign countries [12].

An outbreak of ransomware known as WannaCry struck 150 countries and 40,000 systems in India last year. Ransomware devastated Mumbai's APM Terminal and the Jawaharlal Nehru Port in the same year. In Pune, India, Cosmos bank was hacked in 2018 and hackers took Rs. 944.2 crore from the bank. Due to this, a Hong Kong bank account received Rs 14 crores and ATMs in 28 countries received Rs 80 crores. 1.1 billion UIDAI records were put up for sale by hackers in 2018 after they got access to the government's UIDAI database.

Electrical Power Grid

Attackers can take down vital systems and destroy infrastructure by launching attacks on the power grid. In addition to disrupting communications, attacks on the power grid can also make services like text messages and phone calls unavailable. An attack on the Ukrainian power grid the day before Christmas Eve 2015 resulted in the loss of electricity to approximately half the population of the Ivano-Frankivsk region, which was the target of the attack. As a result of the incident attributed to Russian-based cybercriminals, the globe witnessed the world's first known successful cyberattack on an electric grid. According to the United States Federal Government, United States officials acknowledge that the electric power grid is vulnerable to cyberattacks. The United States Department of Homeland Security collaborates with industry to discover vulnerabilities in control system networks and assist enterprises in improving the security of these networks [13,14]. While developing the next generation of "smart grid" networks, the federal government is working to ensure that safety is built into the design from the outset. Recent reports claimed that China and Russia had hacked the United States' electrical grid and left behind software programs that might damage the system. These claims were made by current and former national security officials and were corroborated by other sources. North American Electric Reliability Corporation (NERC) has published a public notice informing the public that the electrical system is not fully safeguarded against cyberattacks as of yet. China denies that it has interfered with the electrical system of the United States. One possible countermeasure would be to separate the Internet from the power grid and just use droop speed control to operate the network. Massive power outages triggered by a cyberattack might harm the economy, divert attention away from a concurrent military operation, or cause a national crisis.

Iranian hackers, allegedly members of the Iranian Cyber Army, caused a catastrophic power outage that lasted 12 hours in 44 of Turkey's 81 provinces, affecting 40 million people. The cities of Istanbul and Ankara were among those affected by the blackout. In June of this year, Russia announced that a cyberattack by the United States had compromised the country's electrical infrastructure. According to the New York Times, American hackers from the United States Cyber Command inserted malware that could destroy the Russian electrical infrastructure [15].

Propaganda Attacks

It aims to manipulate the beliefs and actions of citizens or soldiers serving in a target country. A country's propaganda can be used to expose embarrassing facts and spread lies to undermine public confidence in the nation's leadership or even side with the nation's enemies. Propaganda on the Internet attempts to maintain control over information in whatever form it takes and influence public opinion. In essence, it is a sort of psychological warfare, except that it is carried out through social media, fake news websites and other digital means. Earlier this year, Sir Nicholas Carter, the British Army's Chief of the General Staff, claimed that this type of attack by players like Russia "is a sort of system warfare that aims to delegitimize the political and social structure on which our military might is founded." As defined by the American Psychological Association (APA), propaganda is the purposeful and systematic endeavor to influence perceptions, alter cognitions and guide behavior to obtain a reaction that advances the desired intent of the propagandist. The Internet has surpassed all other modes of communication in recent years. People may communicate their messages to many people quickly, providing an opening for evil. Terrorist organizations may be able to take advantage of this and use it as a tool to brainwash people. The suggestion has been made that limiting media coverage of terrorist acts will, in turn, reduce the number of terrorist attacks that occur in the future [16].

Economic Disruption

Nowadays, computers are used to run almost all economic systems. Computer networks of financial entities such as stock exchanges, payment systems and banks can be targeted by cybercriminals to steal money or prevent people from obtaining the funds they require. Economic information warfare can have many different forms. It is possible to utilize cyber-attacks to promote or facilitate economic warfare in the context of hyper-connected industrial and business processes. These goals can be met by focusing on a variety of essential infrastructures. Financial and power infrastructure attacks can have severe outcomes.

Table 1: Descriptions of Vulnerabilities [16]

Vulnerability	Descriptions
Software	The utilization of defects in applications or system software might deviate from the original purpose of the software.
Hardware	Hardware can be vulnerable, including microprocessors, microcontrollers, circuit boards, power supplies, peripherals like printers or scanners, storage devices, and communications equipment like network cards. There may be hidden flaws in the intended functionality of these components and opportunities for the introduction of malicious code.
Seams between hardware and software	Reprogrammable read-only memory (firmware) of a computer can be reprogrammed by someone who knows how to do so without permission.
Communication channels.	The communication channels between a system or network and the "outside" world might be exploited in various ways by an attacker. As a countermeasure, an adversary can appear to be an authorized channel user to block its use, jam it or spy on its transmissions to gain information that should remain private and hidden.
Configuration	Consumers can choose between several security and convenience settings in most cases, which the system can adjust. Convenience often takes precedence over security, and as a result, many systems are set up insecurely.
Users and operators	A system or network's authorized users and operators can be deceived or coerced into doing or selling their services to an opponent.
Service providers	Computer services like maintenance and Internet access are frequently provided by third parties in the case of many computer installations. For example, an adversary could try to convince an internet service provider to install malware onto a target computer for them.

This could lead to retaliation from the victim or sympathizers, resulting in a backlash. It may take longer to target commodity value chains, but numerous attack sites exist. It is possible to interrupt the supply of a product by multiple more minor attacks at various points in its chain. However, these attacks may not be linked instantly, so the total size of the attack may go unnoticed. The victim of their friends may not retaliate against a less severe stroke. This decreases the possibility that a victim of a cyber assault will take more aggressive defensive measures, which is in line with the cyber security problem [17].

The use of cyber-attacks in financial information warfare is possible. This can be done in the same way as a typical financial information embargo or by interrupting crucial infrastructure control systems. Commodity value chains underpin much of the world's raw material trade and disrupting them might have a significant economic impact. It's more likely that an attack on the value chain will go undetected since it's slower and more nuanced than, say, an attack on the power grid or a big financial institution. A succession of more minor attacks on various components of the commodities value chain can be used to disrupt the supply chain. The cyber security problem and Porter's Five Forces Model can be used to classify attacks on the commodities value chain as defensive or offensive, depending on the actors involved. However, most categorizations are aggressive, with nothing in defense [18].

Surprise Attacks

These are the cyber equivalents of attacks on Pearl Harbor and September 11, 2001. The goal is to launch an enormous onslaught on the enemy they aren't anticipating, allowing the attacker to damage their defenses and ultimately defeat them. In the context of hybrid warfare, this might be done to create the ground for a physical attack to take place. Because IT systems and networks are subject to cyber-attacks and cyber exploitations, they can occur. As shown in Table 1, most currently existing vulnerabilities were introduced due to design or implementation flaws. As long as countries' military and economic strength are built on IT systems and networks, those systems and networks are vulnerable to assault from the outside.

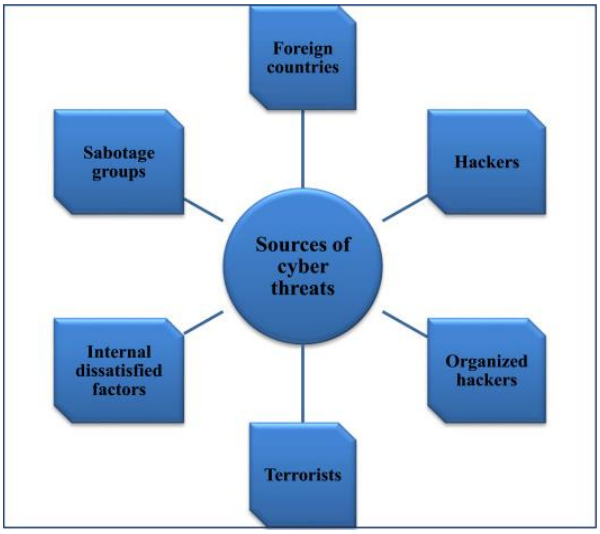

Figure 3: Sources of Cyber Threats [19]

The sources of cyber risks are depicted in Figure 3. Several groups of persons that target cyber systems for financial gain are the source of the attacks and the number of attacks by these groups is increasing. In addition, other groups (hackers) occasionally get access to the network to voice their views. In the current environment, it is possible to enter networks with a minimum of knowledge and abilities by obtaining the appropriate tools and protocols from the Internet and employing them against other websites to compromise their security. Meanwhile, another group (referred to as Hacktivism) with political motivations assaults popular web pages or email hosts on the Internet. It is common for these organizations to increase the burden on email hosts while also infiltrating online sites to broadcast political messages to the general public. Internally dissatisfied agents operating within an organization, on the other hand, are the primary source of cybercrime and these agents do not need to have significant knowledge of cyber-attacks to perpetuate them because their target system awareness typically allows them unlimited access to hit the system or steal information from the organization.

The threat posed by terrorists is another source of concern, as they seek to destroy, disable, or maliciously exploit critical infrastructure to endanger national security, inflict severe losses, weaken the country's economy, undermine public mentality and undermine public trust in the government [20].

CONCLUSION

We may sum it up by saying that cyberwarfare has emerged in recent years and is overgrowing. Many states are launching cyberattacks against governments and other countries using cutting-edge technology. The military's methods of operation have evolved [21]. The military uses a lot of computers and networking technology, which makes them more vulnerable to cyberattacks. On the other side, the military relies heavily on storage and networking technologies, making operations more efficient. They could target a military or government institution, but they also constitute a serious threat. These include a virus, net tracker cyber-attacks, spying and sabotage, sabotaging the electrical power infrastructure and propaganda attacks and surprise attacks and denial-of-service attacks used in cyber warfare. There is no easy way to defend yourself when attacking a computer network. It's normal for these attacks to have little costs for the perpetrators. Still, their effects, eradication and possible prevention are increasingly expensive and may result in billions of dollars in losses. Individuals, businesses, government agencies and the military forces are all victims of such attacks [22]. Destabilizing various infrastructures or critical information infrastructure is among the most severe consequences of a cyberattack. It's tough to catch hackers because of the Internet's anonymity, which is still the most significant issue. When states join in, an even more serious problem will arise.

REFERENCES

[1] Kostyuk, N. and Y.M. Zhukov. "Invisible digital front: Can cyber-attacks shape battlefield events?" *Journal of Conflict Resolution*, vol. 63, no. 2, 2019, pp. 317-47.

[2] Jasim, N.A. and H.TH. "Design and implementation of smart city applications based on the Internet of Things." *International Journal of Interactive Mobile Technologies*, vol. 15, no. 13, 2021, pp. 4-15.

[3] Hruza, P. and J. Cerny. "Cyberwarfare." *International Conference Knowledge-Based Organization*, vol. 23, no. 1, 2017, pp. 155-60.

[4] Azeez, R.A. *et al*. "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique." *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 1, 2022, pp. 178-87.

[5] Salim, H.T. and H.T. Hazim. "Enhanced data security of communication system using combined encryption and steganography." *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, 2021.

[6] Yahya, O.H. *et al*. "Reducing the data rate in Internet of Things applications by using wireless sensor network." *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 16, no. 3, 2020, pp. 107-16.

[7] Estrada, A. *et al*. "Primates in peril: The significance of Brazil, Madagascar, Indonesia and the Democratic Republic of the Congo for global primate conservation." *PeerJ*, vol. 6, 2018, p. e4869.

[8] Watney, M. "Artificial intelligence and its' legal risk to cybersecurity." *European Conference on Cyber Warfare and Security*, 2020, pp. 398-405. Academic Conferences International Limited.

[9] Tabagari, T. "Georgian cyber defense unit." 2016.

[10] Garrison, K. "Examining the true hazards of current and future automobiles." Utica College, 2018.

[11] Greenberg, A. "How not to prevent a cyberwar with Russia." *Wired*, 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/.

[12] Yu, S.Y. *et al*. "Sabotage attack detection for additive manufacturing systems." *IEEE Access*, vol. 8, 2020, pp. 27218-31.

[13] Mar, A. *et al*. "A survey on power grid faults and their origins: A contribution to improving power grid resilience." *Energies*, vol. 12, no. 24, 2019, p. 4667.

[14] Abed, F.T. and I.A. Ibrahim. "Efficient energy of smart grid education models for modern electric power system engineering in Iraq." *IOP Conference Series: Materials Science and* Engineering, vol. 870, no. 1, 2020, p. 012049. IOP Publishing.

[15] Li, Y. and Q. Liu. "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments." *Energy Reports*, vol. 7, 2021, pp. 8176-86.

[16] Khanday, A.M.U.D. *et al*. "Identifying propaganda from online social networks during COVID-19 using machine learning techniques." *International Journal of Information Technology*, vol. 13, no. 1, 2021, pp. 115-22.

[17] Abass, A.Z. *et al*. "Economic feasibility study of a hybrid power station between solar panels and wind turbine with the national grid in Al-Hayy City in the central of Iraq." *IOP Conference Series: Materials Science and Engineering*, vol. 1184, no. 1, 2021, p. 012001. IOP Publishing.

[18] Prihandono, D. *et al*. "SMEs and HEI collaboration: Improving SMEs' performance and knowledge management capability to cope with economic disruption." 2021.

[19] Keshk, M. *et al*. "Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems." *IEEE Access*, 2021.

[20] Otuoze, A.O. *et al*. "Smart grids security challenges: Classification by sources of threats." *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, 2018, pp. 468-83.

[21] Lancelot, J.F. "Cyber-diplomacy: Cyberwarfare and the rules of engagement." *Journal of Cyber Security Technology*, vol. 4, no. 4, 2020, pp. 240-54.

[22] Duddu, V. "A survey of adversarial machine learning in cyber warfare." *Defence Science Journal*, vol. 68, no. 4, 2018, p. 356.