Guarding the Nation: A Comprehensive Look at State Cybersecurity Measure

Marian-Emilian SPĂTARU, Alexandru BARCAN
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
marian.spataru@outlook.com, alexbarcan23@gmail.com

Abstract

In a continuously evolving world, technology has not been left out of the process which consists of studies and research done by specialists in the field of cyber technology. Although the latter has brought along benignant effects in society, it can be considered a controversial domain due to those effects that can be used against the public safety and national security. Cyber-attacks & Cyber terrorism are just two of them, usually countered by Cyber intelligence, OSINT security, Cyber risk management. These actions are coordinated by different intelligence services such as: Federal Bureau of Investigation – FBI, Romanian Intelligence Service – SRI, Federal Security Service – FSB, while they have to cooperate with civilians, due to a shortage of employees. The lack of qualified staff on the following domain: awareness of the different types of cyber-attack, such as malware, web-based attacks, phishing, web application attacks, spam, distributed denial of service (DDoS), identity theft, data breach, insider threat, botnets, physical manipulation, damage, theft and loss, information leakage, ransomware, cyber-espionage, industrial espionage and crypto jacking, reaches an amount of 7.659 officials that are needed in this area.

Index terms: cyber intelligence, OSINT security, cyber-attacks, cyber terrorism, cyber risk management

1. Introduction

State cybersecurity weaknesses refer to the vulnerabilities and the gaps that exist in the cybersecurity defenses of a state. These vulnerabilities and gaps can arise due to several reasons, including inadequate funding, lack of skilled personnel, outdated technology and also poor security protocols.

The major challenge in state cybersecurity is the lack of adequate funding. Many states have limited budgets for cybersecurity, which makes it challenging to implement and maintain robust security measures. As a result, states may have outdated software and hardware systems that are vulnerable to cyber-attacks. The demand of cybersecurity experts has increased significantly in recent years, but the supply has not kept up with the demand. This shortage of skilled personnel can lead to inadequate cybersecurity measures and poor incident response.

So, in order to prevent state cybersecurity weaknesses, governments must allocate sufficient resources to fund and maintain robust cybersecurity measures. All these measures consist of investing in technology, hiring skilled personnel, and implementing best practices for security protocols.

This research aims to provide an overview on cybersecurity of states, how it works, the stages of cyber protection against cyber-attacks, cyber terrorism, and also cyber risk management which also **categorize the levels of risk** [2].

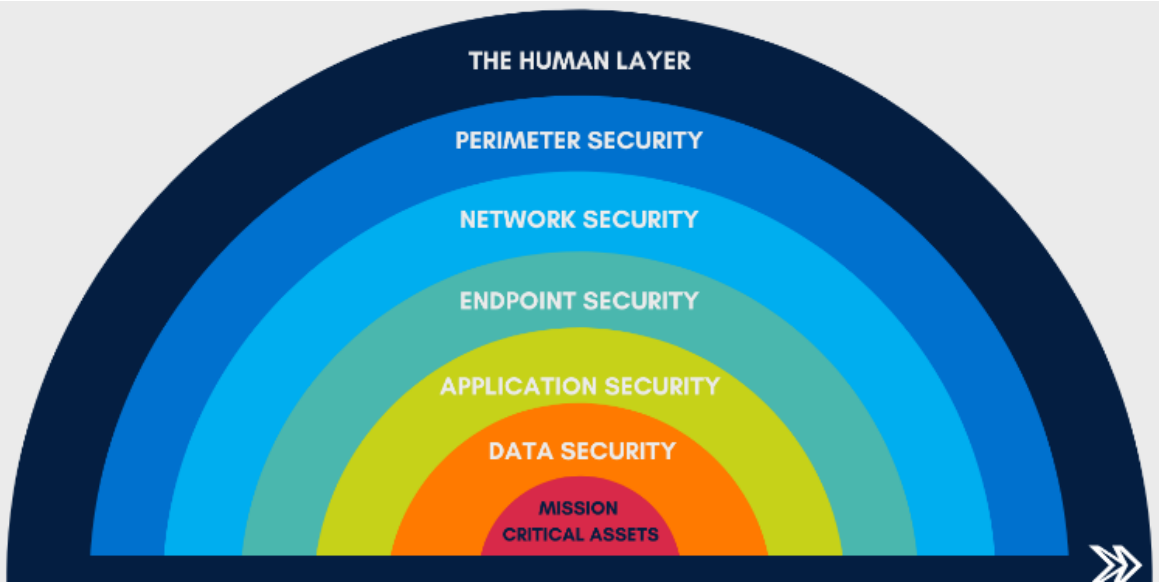

Fig. 1. The 7 layers of cybersecurity (Source: www.diamondit.pro/7-layers-of-cybersecurity/)

2. The Invisible Threat: APT28's Sophisticated Tactics for Hacking and Undermining State Cybersecurity

The hacking groups are divided into two categories:

- **"White Hat"** - In general, "white hat" hackers are individuals who use their technical skills to identify vulnerabilities in computer systems, networks, or applications, with the goal of improving their security.
- **"Black Hat"** - hackers are individuals who use their technical skills to exploit vulnerabilities in computer systems, networks, or applications, for personal gain or to cause harm to others. They are often involved in illegal activities such as stealing data, installing malware, or conducting distributed denial-of-service (DDoS) attacks. Their actions are considered illegal and unethical because they do not have the permission or authorization to perform their activities.

APT28, also known as **Fancy Bear**, is a cyber espionage group that is believed to be based in Russia. The group has been active since at least 2007 and has been responsible for a number of high-profile cyber-attacks around the world. This group is known for using sophisticated and highly targeted techniques to gain access to sensitive information. They have been linked to several attacks on government agencies, military organizations, and political groups in the United States and Europe [11], [14], [15].

One of the group's most well-known attacks was the hack of the DEMOCRATIC NATIONAL COMMITTEE (DNC) during the 2016 US presidential election. The group is believed to have stolen sensitive emails and other data from the DNC and released it to the public in an effort to influence the election. APT28 has also been linked to a number of other attacks, including the hack of the German parliament, the French presidential campaign, and the World Anti-Doping Agency [4].

The group has been known to use a variety of techniques, including spear-phishing malware, and social engineering, to gain access to its targets. The group's motivations are believed to be primarily political in nature, and it is believed to be sponsored by the Russian government. APT28 is considered to be one of the most sophisticated and dangerous cyber espionage groups in the world, and its activities have raised serious concerns about the sensitive information and infrastructure around the world.

The variety of techniques that they use to attack political groups in the United States includes spear-phishing, malware, and social engineering. The techniques are a variety of malware strains,

including X-AGENT and SEDNIT, to gain access to systems and steal data. Once installed on a system, the malware can be used to remotely control the system, exfiltrate data or even carry out other malicious activities. [11], [14], [15].

In the case of the hack of the DEMOCRATIC NATIONAL COMMITTEE (DNC) during the 2016 US presidential election, APT28 used a combination of these techniques to gain access to the organization's systems. The group sent spear-phishing emails to DNC staff members, which contained a link to a fake login page. When the staff members entered their login credentials, APT28 was able to steal their usernames and passwords, giving the group access to the DNC's system.

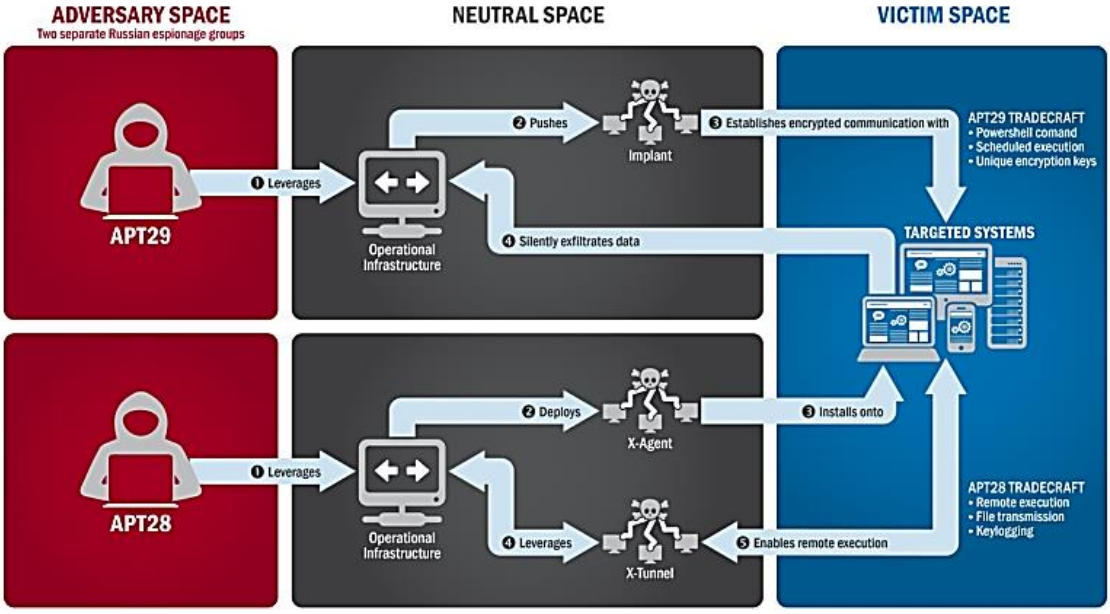

Fig. 2. The tactics and techniques used by APT29 and APT28 to conduct cyber intrusions against target systems

X-Agent and SEDNIT are two malware tools believed to be developed and used by the Russian hacking group known as APT28 or Fancy Bear (diagram taken from [6]).

X-Agent is a remote access Trojan (RAT) designed to give hackers remote access and control over a targeted system. It is capable of performing various malicious activities such as stealing sensitive data, capturing screenshots, recording keystrokes, and executing commands. X-Agent has been used in several high-profile cyber espionage campaigns, including the 2016 Democratic National Committee (DNC) hack [4], [11], [14], [15].

SEDNIT is another malware tool used by APT28. It is a modular malware that consists of multiple components, including a downloader, a backdoor, and a rootkit. SEDNIT is known for its stealthy and sophisticated techniques, such as using anti-debugging and anti-VM techniques to evade detection. Like X-Agent, SEDNIT has been used in various cyber espionage campaigns, targeting government and military organizations, as well as critical infrastructure sectors.

Both X-Agent and SEDNIT are considered highly sophisticated malware tools and are often used by APT28 in targeted attacks aimed at stealing sensitive information and disrupting critical infrastructure [5], [6].

The scientists' research revealed that APT28 utilizes a modular framework called backdoor CHOPSTICK as a means of developing a backdoor. The ironic name is due to its flexibility in compiling variants with different capabilities and the ability to deploy additional capabilities during runtime. With this modular design, the developers can create targeted implants, including only the necessary capabilities and protocols required for a specific environment [5], [6].

CHOPSTICK uses these methods in order to move messages and information:

1. Communications with a C2 server using HTTP.

2. Email sent through a specified email server. One CHOPSTICK v1 variant contained modules and functions for collecting keystroke logs, Microsoft Office documents, and PGP files.

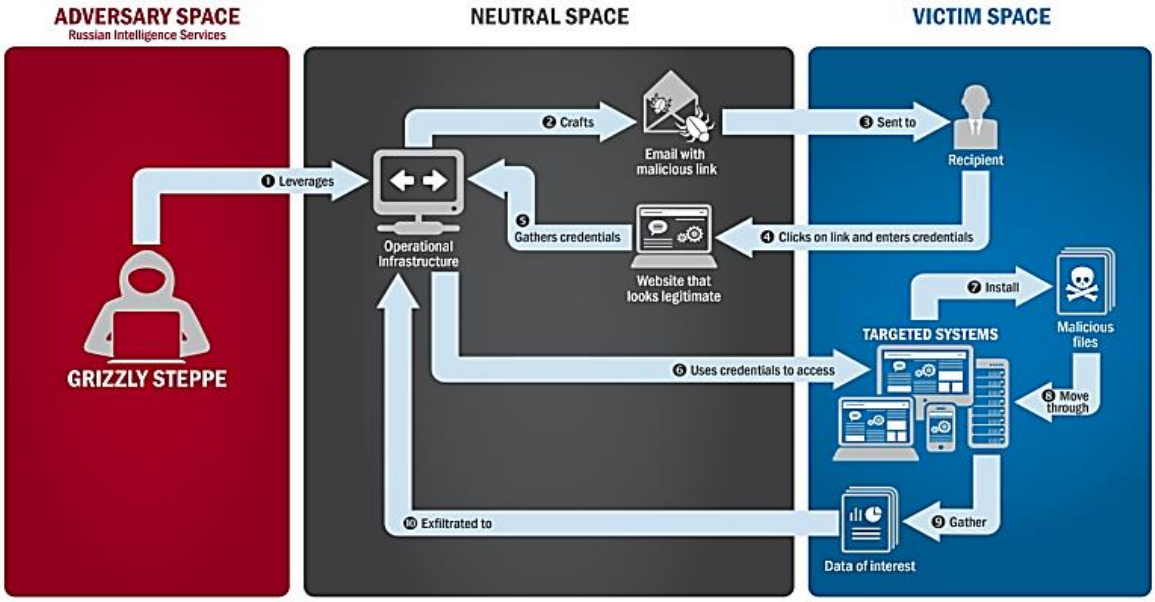

Fig. 3. APT28's use of spear phishing and stolen credentials

Also, during the research, the scientists discovered that APT28 used in the coding two details consistent across the malware samples. The first one was that APT28 had consistently compiled into their malware Russian language settings, which made it harder to read the code sometimes. Also, the second one was the fact that the malware compiled times from 2007 to 2014, and it corresponded with Moscow and St. Petersburg business hours. (Diagram taken from [6])

In conclusion, APT28, also known as Fancy Bear, is a cyber espionage group believed to be based in Russia that has been active since at least 2007. The group is known for using sophisticated and highly targeted techniques, including spear-phishing, malware, and social engineering, to gain access to sensitive information. APT28 has been linked to a number of high-profile cyber-attacks around the world, including the hacking of the Democratic National Committee during the 2016 US presidential election. The group is believed to be politically motivated and sponsored by the Russian government. APT28 utilizes a variety of malware tools, including X-Agent and SEDNIT, to remotely control systems and exfiltrate data. The group also uses a modular framework called backdoor CHOPSTICK to develop a backdoor and communicate with a command-and-control server using HTTP and email. The use of Russian language settings and compile times corresponding to Moscow and St. Petersburg business hours in their malware code indicates APT28's origin and location. APT28 is considered to be one of the most sophisticated and dangerous cyber espionage groups in the world, and its activities have raised serious concerns about the security of sensitive information and infrastructure worldwide [3], [5], [6].

3. Fortifying The Nation: Robust Cybersecurity Protocols for Safeguarding State Security

The idea of fortifying the nation goes above the common sense to fortify something physically. In our field we choose to use," fortify" to refer to the whole action/process which consists of recruiting people to work in the cybersecurity field, training them and gaining advantage in front of other

organisation/states. In this way, we know that the new cybersecurity strategy says that no product is totally secured and cannot be totally secured at least in the near future.

To improve this, new strategies urge the government to consider taking on some responsibility for so-called cybersecurity insurance. It is understandable how many companies and government agencies are reliant on the internet and corporate networks to conduct daily operations. By protecting, or "backstopping," cybersecurity insurers, the administration hopes to prevent a major systemic financial crisis for insurers and victims during a cybersecurity incident. Every country has a National Cybersecurity Strategy institute which is constantly looking forward to doing? continuing research.

Due to the current political situation, with a war ongoing between Russia and Ukraine, the White House led by Joe Biden launched a National Cybersecurity Strategy on March 2023.

The US government is continuingly trying to strengthen the country's cybersecurity safety although its overall technology governance is one of the most powerful in the world.

Earlier that month, President Joe Biden released the new National Cybersecurity Strategy which outlines the steps the government is taking to secure cyberspace and build a resilient digital ecosystem that is easier to defend than attack - and that is open and safe for all [7], [2].

Why does the US need a National Cybersecurity Strategy?

The world is increasingly complex and cyberthreats are growing more sophisticated, with ransomware attacks running into millions of dollars in economic losses in the US. In 2022, the average cost of a ransomware attack was more than $4.5 million, according to IBM.

The greatest risks we face are interconnected, creating the threat of a "polycrisis", whereby the overall combined impact of these events is greater than their individual impact.

This is equally true of technological risks, where, for example, attacks on critical information infrastructure could have disastrous consequences for public infrastructure and health, or where growing geopolitical tensions heighten the risk of cyber-attacks. Cybercrime and cyber insecurity were seen by risk experts surveyed for the World Economic Forum's Global Risks Report as the 8th biggest risk in terms of severity of impact, across both the short term (next two years) and over the coming decade [13].

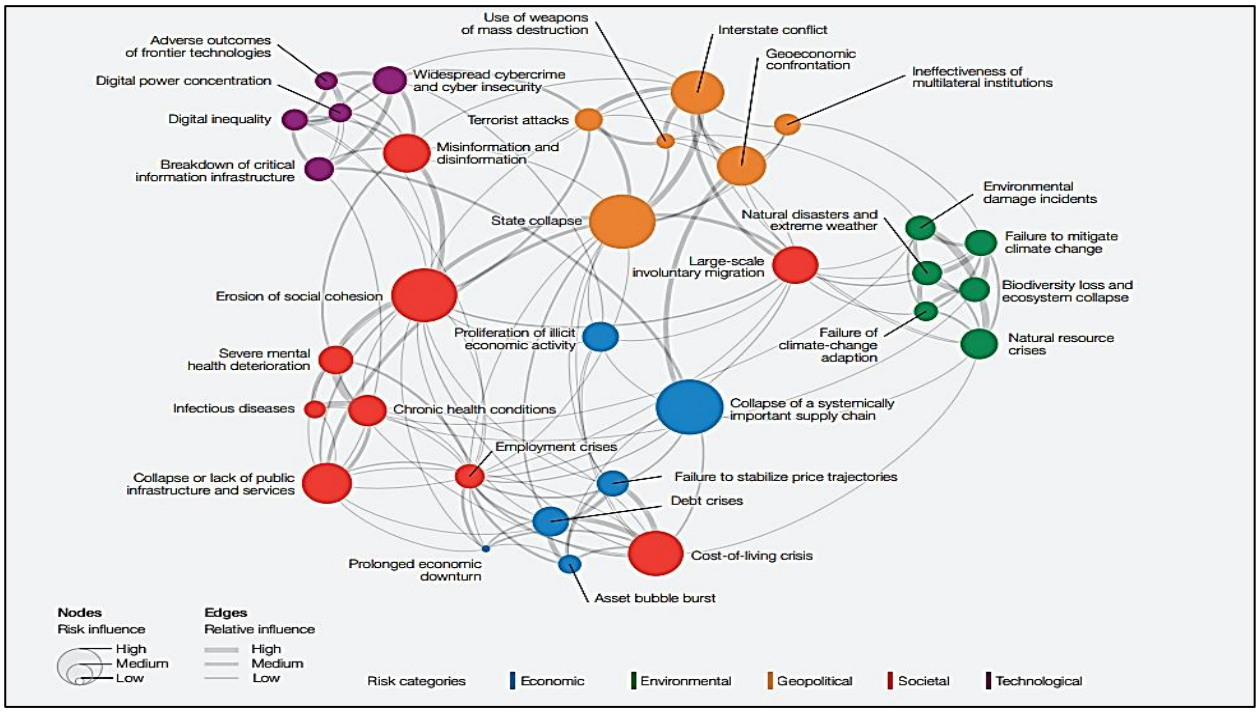

Fig. 4. Google data [13]

In 2022, state-sponsored cyber-attacks targeting users in NATO countries increased by 300% compared to 2020, according to Google data. (Diagram taken from [13])

With cyber-attacks on the rise, experts at the World Economic Forum's Annual Meeting at Davos predicted that 2023 would be a "busy year" for cyberspace with a "gathering cyber storm".

Cybersecurity protocols are the policies, procedures, and guidelines that a state government puts in place to protect its digital assets from cyber threats. These protocols are essential to ensure the security and confidentiality of critical data and systems.

The cybersecurity protocols of a state may include several components, such as access controls, incident response plans, data encryption, network monitoring, and employee training.

Access controls are measures that restrict access to sensitive information and systems to authorized personnel. Access controls can include passwords, biometrics, two-factor authentication, and other security mechanisms.

Incident response plans are procedures that outline the steps to be taken in the event of a cyber-attack or other security incident. These plans may include actions such as isolating affected systems, notifying law enforcement, and implementing backup and recovery procedures.

Data encryption is a technique used to protect sensitive information by converting it into an unreadable format. Encryption can help prevent unauthorized access to data, even if the system is compromised.

Network monitoring involves the use of software tools and techniques to monitor network activity for signs of cyber threats. This includes monitoring for suspicious activity, such as unauthorized access attempts or data exfiltration.

Employee training is a critical component of cybersecurity protocols. Employees are often the weakest link in cybersecurity, and their actions can inadvertently cause security breaches. Effective training can help employees understand the risks of cyber threats and how to identify and prevent them.

In addition to these components, the cybersecurity protocols of a state may also include regular security audits and vulnerability assessments, compliance with relevant laws and regulations, and partnerships with other organizations and governments to share threat intelligence and best practices.

The cybersecurity protocols of a state must be comprehensive, up-to-date, and regularly reviewed and updated to address new and emerging threats. By implementing effective cybersecurity protocols, states can protect their critical data and systems from cyber threats and ensure the safety and security of their citizens.

Another type of cyber-attack

A DDoS (Distributed Denial of Service) attack from one country to another can have serious consequences and is considered a cyber-attack on the targeted country's infrastructure. In a DDoS attack, an attacker typically uses a network of infected computers, known as a botnet, to flood a targeted website or network with traffic, overwhelming its servers and causing it to become unavailable to legitimate users.

A DDoS attack from one country to another can be used as a cyber weapon to disrupt critical infrastructure, such as government websites, financial systems, or healthcare networks. This can cause significant economic damage and impact the ability of the targeted country to function effectively.

In addition to the direct impact on the targeted country, a DDoS attack from one country to another can also have broader geopolitical implications. It can be seen as an act of aggression by the attacking country and may lead to diplomatic tensions or even military conflict.

To prevent DDoS attacks, countries can implement a range of measures, such as using anti-DDoS technologies, increasing network capacity, and improving incident response capabilities. In

addition, international cooperation is important in preventing and responding to DDoS attacks that cross national borders.

Overall, a DDoS attack from one country to another is a serious cybersecurity threat that can have significant consequences for both the targeted country and the broader international community. It is important for countries to work together to develop effective cybersecurity strategies and prevent these types of attacks from occurring [8].

DDoS falls into three types depending on the goal of the attack:

- *Layer Attack* - Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the target's resources to create a denial-of-service.

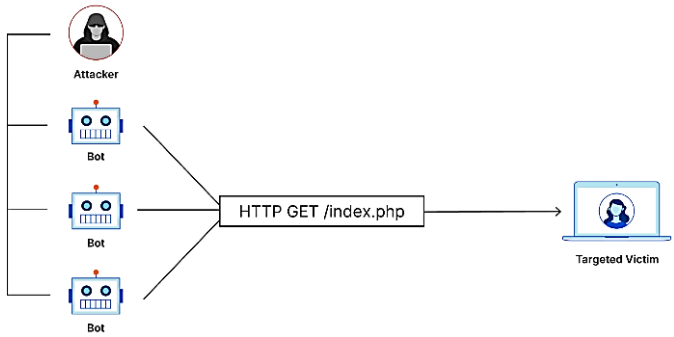

Fig. 5. Layer Attack [8]

- *Protocol Attack* - Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

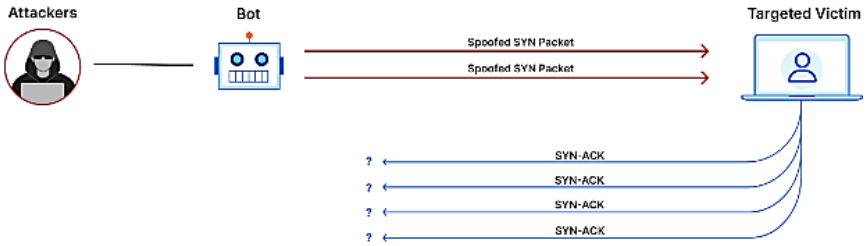

Fig. 6. Protocol Attack [8]

- *Volumetric Attack* - This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

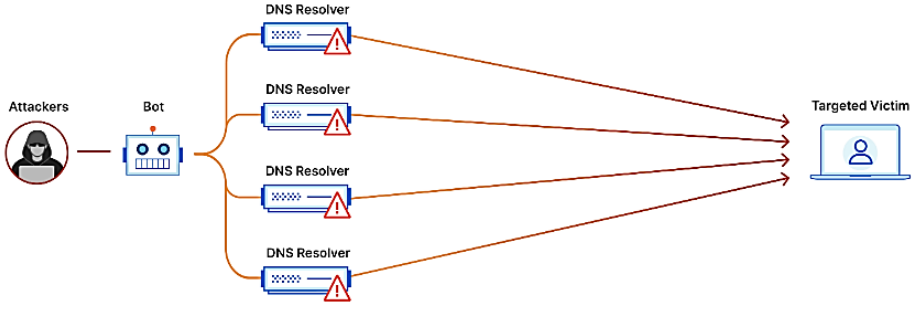

Fig. 7. Volumetric Attack [8]

The 5 pillars of the National Strategy [2] are:

1. Defend critical infrastructure.

To build confidence in the resilience of US critical infrastructure, regulatory frameworks will establish minimum cybersecurity requirements for critical sectors.

2. Disrupt and dismantle threat actors

Working with the private sector and international partners, the US will seek to address the ransomware threat and disrupt malicious actors.

3. Shape market forces to drive security and resilience

Grant schemes will promote investment in secure infrastructure, while liability for secure software products and services will be shifted away from the most vulnerable and good privacy practices will be promoted.

4. Invest in a resilient future

A diverse cyber-workforce will be developed and cybersecurity R&D for emerging technologies including postquantum encryption will be prioritized.

5. Forge international partnerships to pursue shared goals

The US will work with its allies and partners to counter cyberthreats and create reliable and trustworthy supply chains for information and communications technology.

4. Shielding the Nation's Digital Frontline: The Vital Role of the Military

The role of the army in cybersecurity attacks is vital in ensuring the safety and security of a nation's critical infrastructure and sensitive information. The military is responsible for protecting national security interests, which include cybersecurity. As the world becomes increasingly dependent on technology, the military's role in cybersecurity is becoming more important than ever.

One of the primary responsibilities of the military in cybersecurity is to protect the nation's critical infrastructure. This includes infrastructure such as power grids, water treatment plants, transportation systems, and financial institutions. A cyber-attack on any of these systems could have devastating consequences, including loss of life, economic disruption, and damage to the national security.

The military also plays a critical role in defending against cyber threats from other nations or state-sponsored groups. These threats could include attacks on government agencies, military organizations, and other critical infrastructure. The military is responsible for developing and implementing cybersecurity strategies to defend against these threats, as well as responding to and mitigating the impact of successful attacks. In addition to defending against external threats, the military is also responsible for ensuring the cybersecurity of its own networks and systems. This includes protecting sensitive information such as classified documents, personnel records, and communications. The military must also ensure that its own cybersecurity practices are up-to-date and effective, and that its personnel are trained in cybersecurity best practices.

One of the unique aspects of military cybersecurity is the use of offensive cyber capabilities. The military has the ability to use cyber-attacks as a means of disrupting or disabling an adversary's critical infrastructure or communications systems. This type of capability can be a powerful tool in military operations, but it also requires careful consideration and adherence to international law and norms [8], [9].

There are a number of cybersecurity protocols and practices that the army uses in order to protect against cyber-attacks. Here are a few examples:

1. Network Segmentation: This involves dividing a network into smaller subnetworks or segments. This helps to contain a cyber-attack to a single segment, preventing it from spreading throughout the entire network.

2. Firewalls: Firewalls are network security systems that monitor and control incoming and outgoing network traffic based on predetermined security rules. They help to prevent unauthorized access to the network and protect against cyber-attacks.
3. Intrusion Detection and Prevention Systems (IDPS): These systems monitor network traffic for signs of unauthorized access or malicious activity. They can help to identify and block cyber-attacks before they cause damage to the network.
4. Regular Software Updates and Patching: The army regularly updates its software and systems with the latest security patches and updates. This helps to protect against known vulnerabilities and reduce the risk of a successful cyber-attack.
5. Access Control: Access control measures are used to ensure that only authorized personnel have access to sensitive information and systems. This includes the use of passwords, two-factor authentication, and biometric identification.
6. Employee Training and Awareness: The army provides regular cybersecurity training and awareness programs to its personnel. This helps to ensure that all employees are aware of the latest threats and best practices for protecting against cyber-attacks.
7. Incident Response Planning: The army has a detailed incident response plan in place to quickly respond to and recover from cyber-attacks. This includes procedures for identifying, containing, and mitigating the effects of an attack [7].

USA Army is categorised in a list of intelligence gathering disciplines and these are:

- HUMINT
- GEOINT
- MASINT
- OSINT
- SIGINT
- TECHINT
- CYBINT/DNINT
- FININT

These are some of the intelligence categories, working together in order to ensure national state defense.

4.1. Army OSINT: Enhancing Intelligence Gathering with Open Sources

OSINT (Open Source Intelligence) and the army work together in a number of ways to help protect national security and support military operations.

One key area where OSINT can be valuable to the army is in the realm of situational awareness. OSINT can provide real-time information on a variety of topics, including geopolitical events, social media trends, and even weather patterns. By collecting and analyzing this information, OSINT analysts can help the military to better understand the operational environment, identify potential threats, and make more informed decisions.

Another area where OSINT can support the army is in the realm of intelligence gathering. OSINT can provide a wealth of information on a variety of topics, including enemy capabilities, military movements, and other intelligence targets. By collecting and analyzing information, OSINT analysts can provide the military with valuable intelligence that can be used to inform tactical and strategic decisions.

In addition to these areas, OSINT can also be useful in supporting military operations. For example, OSINT can be used to identify key influencers or opinion leaders in a particular region, which can help the military to better understand the local culture and build relationships with key stakeholders. OSINT can also be used to identify potential targets for cyber operations, such as vulnerable computer systems or critical infrastructure.

Also, The US Army is taking the issue of cybersecurity very seriously, as it recognizes the importance of protecting its networks and systems from cyber-attacks. One of the ways the army is combating cyber-attacks is by using OSINT (Open Source Intelligence) to gather information from publicly available sources [7], [9].

OSINT can be used to combat cyber-attacks in several ways. Firstly, it can be used to gather threat intelligence by collecting information about potential cyber threats and attackers. This information can be used to develop threat intelligence that can help the army better understand and mitigate cyber risks. Additionally, OSINT can be used to identify vulnerabilities in army networks and systems, prioritize security measures and remediation efforts, and assist with incident response efforts by providing real-time information about ongoing attacks.

OSINT can also be used to identify potential social engineering attacks against army personnel, such as phishing or spear-phishing attacks. By monitoring social media and other publicly available sources of information, OSINT can provide valuable insights into the tactics and techniques used by attackers to manipulate personnel and gain access to sensitive information.

Moreover, OSINT can help the army monitor the activities of cybercriminals and other malicious actors, including the buying and selling of stolen data and other illicit activities. This information can be used to identify new or emerging threats and to develop effective mitigation strategies to prevent attacks before they occur.

In summary, the US Army is leveraging OSINT to combat cyber-attacks and protect its networks and systems. By using OSINT to gather threat intelligence, identify vulnerabilities, assist with incident response efforts, and monitor cybercriminal activities, the army is better equipped to identify, prevent, and respond to cyber threats. OSINT plays a critical role in the army's comprehensive approach to combatting cyber-attacks and maintaining the security of its information systems.

5. Conclusion

In summary, the role of the military in cybersecurity is crucial in protecting a nation's critical infrastructure and sensitive information, defending against cyber threats from other nations or state-sponsored groups, and ensuring the cybersecurity of its own networks and systems. As technology continues to advance and cyber threats become more sophisticated, the military's role in cybersecurity will only become more important. It is essential that the military stays ahead of these threats and continues to develop and implement effective cybersecurity strategies to keep the nation safe and secure.

References

[1]. Cross-Sector Cybersecurity Performance Goals, March 2023: https://www.cisa.gov/resources-tools/resources/cpg-report.

[2]. Boozallen, What are the 7 types of security? https://www.boozallen.com/expertise/cybersecurity/national-cyber-strategy.html.

[3]. ESET, Part 1: “En Route with Sednit: Approaching the Target” Part 2: “En Route with Sednit: Observing the Comings and Goings” Part 3: “En Route with Sednit: A Mysterious Downloader”, October 2016: https://www.eset.com/afr/about/newsroom/press-releases-afr/research/dissection-of-sednit-espionage-group-1/.

[4]. Editorial Team from Front Lines, CrowdStrike’s work with the Democratic National Committee: Setting the record straight , 5 June 2020: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[5]. Malpedia, X-AGENT & MALWARE Reports, 2014-2020: https://malpedia.caad.fkie.fraunhofer.de/details/win.xagent.
[6]. CISAGOV & FBI, X-AGENT MALWARE FAMILY (Figures&Working Diagram), 29 December 2016: https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
[7]. World Economic Forum, Global Risk Reports, January 2023: https://www.weforum.org/reports/global-risks-report-2023/.
[8]. Cloud Flare, DDoS Attacks: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.
[9]. The importance of cybersecurity in military, Nicole Allen, 20 Oct. 2021: https://saltcommunications.com/news/the-importance-of-cybersecurity-in-military/.
[10]. Fireeye APT28 & Programing Lines: http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf.
[11]. National Security Technology Accelerator, 26 April 2022: https://nstxl.org/cybersecurity/.
[12]. Akshay Joshi, Daniel Dobrygowki, World Economic Forum, The US has announced its National Cybersecurity Strategy: Here's what you need to know, 9 March 2023: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/.
[13]. Cyberscoop, Christian Vasqyez, 16 December 2022: https://cyberscoop.com/apt28-fancy-bear-satellite/.
[14]. Editorial Team, Research & Threat Intel, Who is FANCY BEAR, 12 February 2019: https://www.crowdstrike.com/blog/who-is-fancy-bear/.