ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of Cyber Threats Cape

Mr. Bhavesh Neekhra,
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India
Email Id-bhavesh.neekhra@presidencyuniversity.in

Abstract: ***The "Cyber Threats Cape" is a thorough framework created to defend persons and organizations against the constantly changing world of cyber-attacks. To protect important resources and data, this novel strategy combines cutting-edge technology, clever algorithms, and proactive defense techniques. The Cyber Threats Cape ensures minimum impact and maximum resilience by analyzing real-time data and using machine learning capabilities to give early detection and quick reaction to new threats. This framework gives users the ability to safely traverse the complicated digital world thanks to its multidimensional approach and ongoing monitoring, strengthening the cybersecurity posture and promoting a secure and reliable online environment. The threat landscape is often understood to include the vulnerabilities, malware, particular attack groups, and attack methods that provide a risk in a certain situation.***

Keywords: Cyber Security, Cyber Threats, Confidentiality, Internet, World Wide Web.

INTRODUCTION

The early 1980s saw an emphasis on interoperability and dependability as a method of communication and possible command and control in the case of an emergency. ARPANET was evolving into the World Wide Web, which expanded into today's Internet. Security was not a concern since everyone who had access to the system was familiar with one another. Then, in the late 1980s, problems began when Clifford Stoll uncovered Soviet Block spies collecting US secrets via a mainframe at the University of California, Berkeley, and Robert Morris published the first worm, a self-replicating piece of malware. These were swiftly followed by many events that illustrated the security vulnerabilities connected to our new communication capabilities [1].

The 1998 Solar Sunrise incident made headlines as the Pentagon was hacked when America was at war with Iraq, but the instigators were two youngsters from California. These major events as they pertain to and have an influence on the military happened in the mid-to-late-1990s when Time magazine featured a cover on "Cyber War." Hackers often choose to route their assaults via nations that won't help with an inquiry, as was the case with Moonlight Maze, when the Department of Defense (DoD) discovered intrusions from systems in the Soviet Union (though the source of the attacks was never proved) and Russia denied any participation. By the beginning of the new millennium, a string of assaults known as Titan Rain were identified as coming from China. After the media revealed the Titan Rain code name, the name was changed to Byzantine Hades. It was then altered once again after the Byzantine Hades code name was leaked to WikiLeaks. The phrase "Advance Persistent Threat (APT)" has started to be used interchangeably to describe to this state-sponsored electronic snooping and digital espionage. The entropic assaults had a physical component by the late 2000s, which the DoD code-named Operation Buckshot Yankee. Due to the discovery that US Military thumb drives had embedded malicious malware; DoD banned the use of thumb drives on all military networks and systems. In the 2000s, there were other international occurrences besides assaults against US military targets. 2007 saw the takedown of the websites for Estonia's parliament, banks, ministries, newspapers, and broadcasters by hackers thought to be affiliated with the Russian government.

NATO agreement for defense and soldiers to aid in recovery. A year later, amid a military crisis with Russia, cybercriminals in Georgia seized official and commercial Web sites, launching a brand-new kind of online digital signal jamming. Finally, in 2010, the StuXnet worm targeted and damaged the systems that oversee Iran's nuclear material production. Other significant occurrences mirror the struggles of the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

military. According to allegations from 2009, hackers acquired information from the DoD's expensive F-35 Joint Strike Fighter program, demonstrating that they were targeting both defense companies and the military as targets. Then, in 2010, Operation Aurora made headlines when Google announced that it was one of several for-profit organizations that the APT had breached, demonstrating that the hackers were also pursuing commercial intellectual property. In 2011, there were two alarming assaults. The first was a string of cyberattacks revealed in the "Night Dragon" global energy report, which demonstrated China's attempts to use espionage to obtain a competitive advantage in the energy sector. The second was the RSA assault, which demonstrated that the adversary was prepared to target the infrastructure used to safeguard the US by allowing a hacker to duplicate the number that appeared on the password token many organizations used to secure their networks [2].

Defenders and attackers from networks all around the world have been engaged in a never-ending conflict for the last 30 years. In many circumstances, the attacker is just interested in acquiring as many systems as they can, regardless of whether the target is a military, government, or commercial organization. The cycle continues as new assaults and solutions are created. Some people will see J.R.'s Mordor map. The map is actually intended to show the resources and tactics the attackers (second column) will use to try to get past the defenses built into the mountain range in order to reach the valuable data they are seeking on the far side (far right side) of Tolkien's fictional Middle-Earth, which is what others see as the Ponderosa.

Attack Methodology Plus Tools/Techniques Used

It becomes clear when we investigate how networks are breached that the fundamental phases in the process are comparable to conventional military attack/defend doctrine. Demilitarized Zone (DMZ), similar to the actual border between South and North Korea, is the phrase used by network administrators to describe how defending forces construct defense in depth. On the assaulting side, attackers conduct reconnaissance, deploy troops at the enemy's weak spot, launch an attack, and take advantage of penetration.

The weaponry vs. software programs they use are the primary distinction between Kinetic (real world) and non-Kinetic (virtual world) combat methodologies. In order to clarify some of the instruments utilized, we shall go through the processes. This is only to get a general knowledge of the tools; other chapters will go into more depth. Attack methodology refers to the broad procedures or stages utilized to attack a target, as well as any prospective instruments or tactics that may be used. Attack, exploit, and recon are the three main phases. These actions may take many different forms, such as conducting machine-to-machine assaults or using social engineering. Consider social engineering as tricking someone into providing information so that a hacker may breach a network. Each of these processes or phases requires a number of supporting actions to be completed, and many hackers often automate and adapt these steps to fit their own preferences [3].

A target is necessary to start the recon phase. The persons using them or the particular systems that will be targeted might serve as the target. The specific Internet Protocol (IP) address of the device or the Uniform Resource Locator (URL) of the Web page must be known in order to attack the devices. A phone number is often all that is required to launch an attack via the users. You can quickly get IP addresses and phone numbers using Google or via sites like American Registry for Internet Numbers (ARIN) searches. On a business card, you may find a lot of the information required for a social engineering assault.

Once the target has been located, the recon process starts to look for a weakness or opening. The operating system or one of its apps (such as Adobe Flash, Microsoft Office, Games, Web browsers, or an instant messenger) may be the target of the assault. The system is subjected to a scanner, which identifies and lists many of the vulnerabilities. Nmap, Nessus, eEye Retina, and Saint scanner are a few of the most well-known scanners. There are attack framework tools that can scan an application for vulnerabilities and then launch attacks using the corresponding exploits. Metasploit, Canvas, and Core Impact are some examples of well-known framework tools. The last utility is one that uses a LinuX live CD to boot a computer into a LinuX system. BackTrack is the most widely used live CD attack tool.

A sniffer is yet another device that comes in handy during recon. This technique allows the attacker to capture all network communication by having the attacker's machine act like every other computer. The hacker will be able to see the Web sites that everyone on the network is accessing as well as read any emails

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

and documents that are not encrypted. The sniffers Wireshark, Ettercap, and Tcpdump are well-known. The wireless tools Aircrackong and Kismet [4] are examples. While there are many strong and user-friendly recon tools, packet crafters are the one collection of tools that best illustrates how the threat landscape has changed. Now, even someone without programming knowledge may create original assaults. NetCat and Hping are common tools. Although there are many more recon techniques available, they serve as the foundational tools for finding the weaknesses that enable transition to the attack phase.

There are numerous different kinds of malcode that may be utilised while attacking a system. At the code level, worms and viruses are capable of installing rootkits or Trojan horses that serve as backdoors into systems and are used to propagate an attack. These attack vectors include cross-site scripting (XSS) and buffer overflows. A worm spreads on its own. While a virus requires human input, such as opening any form of file like e-mail, document, presentation, or running a program like game, video, new app, it infects a system and uses it to discover additional systems to propagate to. In order to compromise the code, worms and viruses employ strategies like cross-site scripting or buffer overflows. A Web-based assault known as cross-site scripting enables unauthorized code to be performed on the viewer's computer, which may lead to the theft of information or the system's identity certificates. When a program asks for a phone number, an oversimplified example of a buffer overflow is when the software sends 1000 digits instead of the required 10 digits, followed by a prompt to install the malicious malware. The program runs the malicious code because it has poor error handling. A rootkit is a piece of software that seizes control of the operating system and fabricates information about what is occurring there. Once a rootkit is installed, it can misdirect applications (such as showing antivirus software as regularly updated but preventing it from doing so) and hide the hacker's folders (such as hacker tools, illegal movies, and stolen credit card numbers) or misrepresent the status of the system (such as leaving port 666 open so the hacker can remotely access the system but showing it as closed).

The first generation of rootkits, known as the "fibbing 4s" since that's when most kids start learning to lie, was quite similar to my daughter when she was four. The initial generation of rootkits did not lie as effectively as a four-year-old. The age we are in today is more similar to the one she was in when she was 21 because she was MUCH more adept at constructing a convincing tale that was difficult to distinguish from a lie. The ability of the most recent rootkits to evade detection has greatly improved. The next generation will be almost undetected, like someone with a master's in social engineering. A Trojan horse backdoor is a program that poses as a trustworthy file, often a system file, such as the system library on a Mac or files ending in.sys on Windows. These files have really taken the place of the genuine system file and are forgeries. The new file allows the hacker to remotely manipulate the machine while also enabling the system to operate.

The creation of botnet armies is one usage for worms and viruses. A computer that is under the control of another person is referred to as a boat or zombie. Once a person has amassed a massive bot army, they may launch a distributed denial of service (DDoS) attack by having every single one of the bots attempt to connect to the same website or system at once. This can be done to disrupt command and control systems, engage in click fraud for example, if Acme.org is paid one cent for each customer who clicks on a link that takes them to Selling.com, a botnet could be used to perform that action millions of times per day or compile complex problems in a manner akin to a distributed supercomputer [5]. Instead of casting a wide net as a worm or virus would, there are a variety of techniques to launch attacks that are tailored to a particular machine. The most prevalent are the already described attack framework tools. Correlating the exploit to the vulnerability is crucial. Similar to how no bank has ever been constructed that cannot be stolen, no computer or network can be breached without sufficient resources and perseverance. If there is no vulnerability, the attacker may attempt to compromise the authentication process through credential or password assaults.

By having a computer attempt every iteration of a password, brute force may be used to crack passwords. Depending on the strength of the password, this may be quite successful but takes time and is detectable. Tools like Cain & Able or Jack the Ripper may be used to break passwords if the hacker has access to the password file. Rainbow tables is another method that is accessible. These are databases where every key combination on a typical keyboard has been tested using well-known password encryption algorithms.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

When a hacker has access to the list of encrypted passwords, this precompiled list enables a quick query. Many of these tables support every possible combination for 8–20 characters, and as hackers continue to employ botnets to construct the tables, their length increases.

In the exploit stage, the attacker uses a weakness to seize power. The hacker may often undermine one of three things: availability, confidentiality, or integrity (CIA). They are only stealing secrets when they violate confidentiality. Integrity attacks occur when someone modifies data stored on the system. This can include modifying client information or pricing in a business situation. It could be necessary to alter the equations used to determine command and control guidance on a military network. Attacks on availability are often time-based and may be carried out by overloading the bandwidth or bringing the system to a halt. The motives of the attacker determine the sort of exploit. They may impersonate the user (send bogus emails), use the system to target further computers on the network, or install a rootkit with a backdoor to keep access for a long time. They will often make an effort to remain undetected and may even use anti-forensic strategies like log erasing and time stomping. Some people may patch the system to prevent intrusion and theft from others. Finally, to let them know if they have been discovered, they may load digital tripwire alarms.

Social engineering is yet another assault method. Although it may be done in person, calling is usually the preferred method. It might include doing research on a company's website, using social media, and meeting individuals in person to trade business cards at events like conferences. Today, email-based attacks are the most frequent. Phishing, spear phishing, and whaling are all terms used to describe this kind of social engineering assault that targets a senior member of the organization. Phishing involves sending generic emails to several recipients. Technical aids for attacking the workforce include the "Social Engineer Toolkit" and other similar tools.

Attackers (The Types of Threats)

The many types of attackers will be the main topic of this section. As we examine the threats cape map, we see that there is no specific ranking or ordering of the attackers. It is essential to remember that even if there are solid lines separating them, they may also miX and overlap. One particularly unsettling paradigm shift that has occurred recently is that hacktivists can act like insider threats while they steal information and then publish it on websites like WikiLeaks. The Advanced Persistent Threat (APT) can purchase exploits from criminal elements. Novices can join hacktivist causes [6].

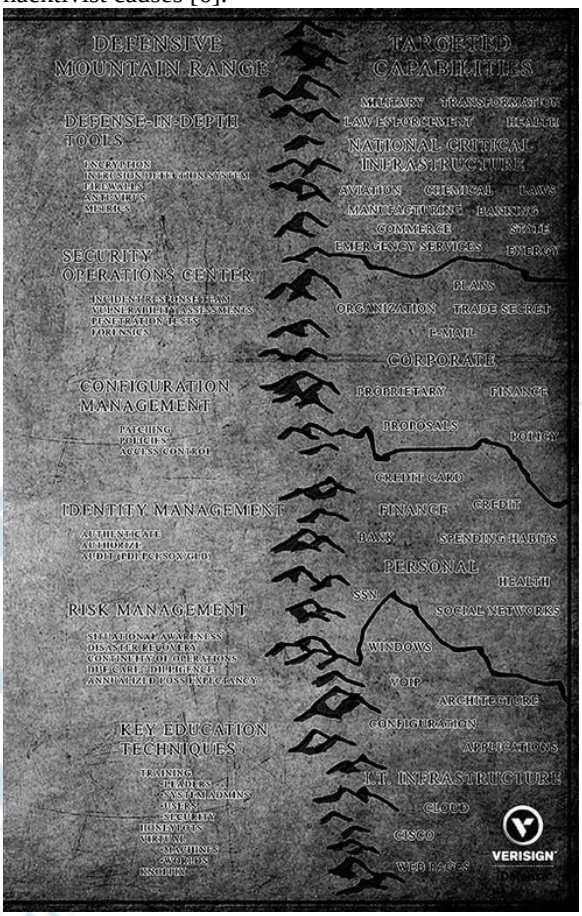

Figure 1: Threats cape Designed to Show the Different Components in the Cyber. Environment

One of the main forces behind cyberwarfare is APT. Although the media often uses the word "APT" in a variety of contexts, for the purposes of this book, APT refers to state-sponsored assaults. In the virtual realm, it is actual digital espionage. A few of the most often cited activities were covered before. The "Global War on Terror" and the "War on Drugs" that the US is waging now have a lot in common with the Cold War. Political allusions to economic warfare are also present; they may be more suitable for these actions. Although China or Russia is usually mentioned in connection with assaults, it's crucial to keep in mind that the cost of entry makes cyberwarfare appealing to all countries. Entry is inexpensive, and the likelihood

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

of any serious repercussions is minimal.

The next subject is organized crime on the Internet. The "Nigerian royalty that just needs access to your bank account" fraud, which sends phishing emails aimed to steal identities and access the victims' bank accounts, is one of the most often made fun of scams on the Internet. The scammers from Nigeria would claim in the emails that they have money that they need to transfer to a US bank in order to leave the country, but they require access to the victim's account in order to accomplish so. Since the offenders are often located abroad, it is now simpler to carry out these frauds in large quantities and with minimal fear of being imprisoned than it was before the Internet. Selling counterfeit medications is a common fraud. While some of the websites offer genuine medications, the majority if they ship anything at all will provide phony medication. These same tricks may be used to persuade personnel of the armed forces or the national security apparatus to engage in actions that they would not normally conduct [7], [8].

Political opinions, cultural or religious convictions, feelings of patriotism, or terrorist ideologies may all inspire hackers. The most recent instance came from a group going by the name of Anonymous. This international network of loosely associated hackers came together to target companies they believed were at fault. In 2008, this online vigilante group launched an assault against the Church of Scientology under the project name Chaology and began using the phrase "We are Anonymous." This is Legion. We don't pardon. We never forget. Consider us. The Bay Area Rapid Transit system (in response to their closing down cell phone tower coverage at the stations to prevent a protest), Sony (in response to a law suit they brought), HBGary Federal (in response to statement made by Aaron Barr), Law Enforcement Agencies for policy they do not support, Political Parties, and many Government sites around the world have all come under attack. Many of their fans are often seen donning Guy Fawkes masks from "V for Vendetta."

DISCUSSION

The Russian Business Network (RBN), sometimes known as the Russian Mob notice that this is not a single organization, is one of the most well-known criminal organizations. One of the better-paying positions available to computer science graduates from universities in the former Soviet Union block nations is with the RBN. They will devote their whole time to creating specialized exploits there that target certain financial institutions, creating legions of bots, managing networks for identity theft, or any one of a hundred other "business ventures" for them. It is incredibly difficult to prosecute these organizations if they are found since they are staffed in one nation, utilize systems hosted in another country (for a time, they used systems in China), and conduct crimes against people in a third. Aside from "Fatal System Error" by Joseph Menn, another book on the topic and one that also uses the RBN as an example is "Fatal System Error." The US has revealed comparable actions, so Russia is not the only nation with cyber-based criminal organizations. In numerous publications, the adage "insider threats represent 20% of the threat but could cause 80% of the damage" is said; nevertheless, new research indicate that the actual percentage of insiders is closer to 50%. The reason is because insiders are aware of the network's valuable assets and often have access to them. Insiders may be divided into three main categories: resentful workers, financially motivated individuals, and inadvertent users. By disgruntled workers disclosing information to other businesses or their own coworkers online, issues might arise. Insiders with financial motives may abuse business resources or game the system to steal. They may also place a logic bomb that will inflict harm if they leave the organization (for example, reformatting all servers in the data room if Winterfield is no longer listed as an employee). Users may also accidently destroy data, which results in lost work, or they may accidentally put classified papers on systems that are not classified, which results in a spill. Spills can need system damage and a protracted inquiry [9]–[11].

CONCLUSION

Many of Anonymous' leaders have been detained by the FBI as of early 2012, but more of these organizations are likely to emerge. The less experienced hackers are derisively referred to as script kids or noobs. These are the people who are limited to using online resources' tools. There are several reasons to begin hacking. Some people try to join hacker groups in search of a social experience, though some groups demand proof of hacking prowess before admitting new members. Others enjoy the challenge or want to advance their status within the hacker community. Still others do it out of curiosity and view

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

it as entertainment. The issue these script kids bring to the cyber warfare scene is the volume of activity they create, which we can see numerous instances of at hacker conferences like DEFCON and HOPE. How can the APT or particular criminal activities be found if millions of attacks each week are conducted by newbies? It's also critical to recognize that they will end up PWNing (slang for owning) systems because of the tools they utilize, which are quite potent. The Defense Information Systems Agency (DISA) has consistently stated that the majority of systems compromised were from known exploits that could have been prevented if the systems were fully patched and configured to standard, and the old adage "the defender has to get it right every time while the attacker only has to get it right once" applies here.

REFERENCES

[1] S. Winterfeld, “Chapter 1 - Cyber Threatscape ,” in The Basics of Cyber Warfare , 2013.

[2] J. Andress and S. Winterfeld, “Cyber Threatscape,” in Cyber Warfare, 2014. doi: 10.1016/b978-0-12-416672-1.00002-7.

[3] A. Roberts, Cyber Threat Intelligence. 2021. doi: 10.1007/978-1-4842-7220-6.

[4] J. Andress, S. Winterfeld, J. Andress, and S. Winterfeld, “Chapter 2 – Cyber Threatscape,” in Cyber Warfare, 2014.

[5] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G.-J. Ahn, “ ExSol ,” Digit. Threat. Res. Pract., 2021, doi: 10.1145/3428156.

[6] P. Duvenage and S. Von Solms, “The case for cyber counterintelligence,” in IEEE International Conference on Adaptive Science and Technology, ICAST, 2013. doi: 10.1109/ICASTech.2013.6707493.

[7] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn, “ExSol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems,” Digit. Threat. Res. Pract., 2021, doi: 10.1145/3428156.

[8] S. Winterfeld, “Cyber Threatscape,” in The Basics of Cyber Warfare, 2013. doi: 10.1016/b978-0-12-404737-2.00001-x.

[9] P. Duvenage and S. Von Solms, “Putting counterintelligence in cyber counterintelligence: Back to the future,” in European Conference on Information Warfare and Security, ECCWS, 2014.

[10] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn, “ExSol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems,” in 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2019 - Held as part of CPS Week, Proceedings, 2019. doi: 10.1109/MSCPES.2019.8738791.

[11] B. T. Contos, “Cyber Crime and Cyber Criminals 101,” in Enemy at the Water Cooler, 2007. doi: 10.1016/b978-159749129-7/50006-0.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Organizations Defend Cyber Security

Mr. Naina Mohamed Zafar Ali Khan
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-zafaralikhan@presidencyuniversity.in

Abstract: ***The Significance of Organizational Efforts in Cybersecurity Defense" is a comprehensive investigation that examines the crucial role organizations play in defending against cyber threats and protecting digital assets. Given the growing reliance on technology and the increasing complexity of cyberattacks, this research emphasizes the importance of strong cybersecurity measures and collaborative actions necessary to counter the constantly evolving threat landscape. The study explores diverse strategies employed by organizations, such as proactive risk assessment, the implementation of advanced security controls, and the cultivation of a robust security culture among employees. Moreover, it delves into emerging technologies and trends that shape the cybersecurity landscape, such as artificial intelligence and machine learning, while also addressing the challenges organizations face in maintaining effective cyber defenses. By illuminating the significance of organizational initiatives in countering cyber threats, this research offers valuable insights and practical recommendations for enhancing cybersecurity resilience in the digital era.***

Keywords: Cyber Attack, Cyber Security, Identity Management, Organization, Security Management

INTRODUCTION

The Defensive Mountain Range depicted on the threat's cape map represents the various methods utilized for safeguarding networks in present times. It encompasses the infrastructure and procedures employed to secure systems and identify any unauthorized access. Similar to physical defenses, these measures require continuous validation, monitoring, and updating. Most networks rely on Defense-in-Depth, which involves implementing multiple layers of protection. However, the proliferation of mobile devices (laptops, phones, tablets) and removable storage media poses a challenge in maintaining a secure perimeter around all systems. Several essential tools are utilized in this regard, including firewalls to block attacks, intrusion detection systems (IDS) to provide alerts about attacks, antivirus software to neutralize successful attacks, and encryption to secure data on devices, thereby ensuring its safety even if the device is lost or stolen. A crucial aspect is the implementation of effective security metrics. These metrics aim to quantify the impact of cyber events and support both technical and senior leadership in making informed decisions to protect the network. They also aid in responding to changes in risk assessment and understanding the return on investment in security infrastructure. While considerable efforts have been made in this area, there is currently no universally accepted set of industry standard cyber metrics. Generally, three main types of metrics exist, providing different perspectives and insights [1]:

i. **Technical:** Based on infrastructure and the incident response cycle.
ii. **Security return on investment (ROI):** Cost-based analysis on benefits from implementing new technology or policies. These goals must be set before they change and methods to track performance are established.
iii. **Risk posture:** Analysis on impact of cyber events/incidents to enterprise and operations.

Following the defensive measures, there is a designated cell responsible for monitoring the network, often referred to as the Security Operations Centers (SOC) or Computer Emergency Response Team (CERT). These cells typically include Incident Response Teams that handle the Protect, Detect, React, and Recover phases of the response cycle. This cycle is analogous to the military's OODA Loop

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

(Observe, Orient, Decide, and Act). The SOC's duties also encompass conducting Vulnerability Assessments (VA) and Penetration Tests (PT). The VA aims to identify network vulnerabilities and prioritize their mitigation or resolution. On the other hand, the PT evaluates the team's ability to respond to an intrusion. Depending on the scope and interaction between the parties involved, Penetration Tests may also be referred to as Red Teaming. During PT, the team attempts to exploit identified vulnerabilities, gaining access to the system and either retrieving a pre-determined file (known as the flag) or uploading a file onto the system (known as the golden nugget). Subsequently, the SOC team must analyze how the PT team infiltrated the system and their actions. This validation process ensures the effectiveness of the team's processes and tools. Following an intrusion, a crucial capability required is that of a forensics expert. This individual possesses a deep understanding of evidence rules and can provide testimony in a court of law. Forensic analysis plays a pivotal role in comprehending the incident and taking preventive measures to avoid its recurrence.

Configuration Management

Configuration Management plays a crucial role in defense operations. A securely configured and well-managed network enhances overall security. To illustrate, imagine approaching a cruise liner for a vacation and discovering it covered in rust, making it impossible to determine its original color. It would be common sense not to board such a ship. However, we often overlook the fact that our network devices may be outdated, just like the rusty ship, and still store our most valuable information. To address this, it is essential to adhere to the basics, such as timely patching. Before installing patches on critical operational systems, thorough testing is necessary. Determining the appropriate time for analysis poses a challenge, with some suggesting a 72-hour window. However, this timeframe can be costly, so there is flexibility in deciding the timeframe. Having well-established and enforced policies for both users and network administrators is imperative. Their decisions regarding operations or processes can influence the security baseline, but they often fail to consider the impact on security risks. Lastly, access control must be effectively managed, granting access to mission-critical data only to authorized individuals. This can be accomplished through physical means or electronic policies. Known as the principle of least privilege, this practice has been employed by the intelligence community for several decades [2].

Identity Management

Identity Management is an essential aspect that will be beneficial as users become increasingly mobile. The key elements involved are authentication, authorization, and audit/compliance. Prior to accessing the system, individuals should provide proof of their identity through three factors: something they know (such as a username and password), something they possess (such as an electronic token), and something they do (biometrics, like scanning a fingerprint). This process is known as authentication.
Furthermore, users should be categorized based on the type of information they are permitted to access. While the military employs the classification system of Unclassified/Secret/Top Secret, various organizations have developed their own systems.
Lastly, considering that every network is susceptible to vulnerabilities over time, it is prudent to assume that unauthorized access may occur. Therefore, conducting regular audits is crucial to identifying any breaches or infiltrations. Compliance with legal and regulatory requirements is also a key aspect. Various industries have specific regulations to adhere to, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, the Gramm-Leach-Bliley Act for finance, the Sarbanes-Oxley Act for publicly traded companies, the Payment Card Industry for credit cards, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program for energy providers, the Federal Information Security Management Act (FISMA) for federal agencies, the Director of Central Intelligence Directive (DCID) 6/3 for the US Intelligence Community (IC), and the DoD Information Assurance Certification and Accreditation Process (DIACAP) for the US Military. Although most of these regulations currently rely on annual system reviews, there is a shift towards real-time monitoring.

Risk Management

All of these laws have been geared towards risk management. Realizing Situational Awareness (SA) is the objective. Decision-making is made possible through SA, which is the correlation and fusion of data from several sources. The best way to display it is graphically using Common Operational Pictures (COP), which will help people comprehend the real risk posture and provide them the data they need to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

make choices. The Disaster Recovery (DR) and Continuity of Operations Plans (COOP) are activated in the event that the network is lost. While COOP is the strategy to go on with no automation, DR concentrates on restoring the network [3].

It is crucial to realize that there are legal requirements on how the network will be safeguarded when we develop systems and networks. Due diligence and care are terms used to describe these ideas. Based on the formulas for "Annualized Loss Expectancy" (vulnerability x threat x asset value = total risk, total risk x countermeasures = residual risk), these estimates should be used. By defining the requirements, designing and developing the protective measures, implementing and validating the defensive solution, operating and maintaining risk management controls, it will be possible to assess where the organization is in the security lifecycle. As a result, security may be built into the system rather than being added afterwards, which is always more costly and less effective.

Education that aims to change users' behaviors is one of the best protective strategies. The training needs to be tailored to the various user types: leaders need to learn how to manage cyber risk, system administrators need to comprehend the value of configuration management and patching, everyday users must learn how their actions can create security flaws that hackers can exploit, and the cyber security team must be aware of the most recent threats and defense tools/techniques. Honeypots, virtual machines, virtual worlds, and live CDs are a few helpful tools. Systems that are installed but have no operational purpose are called honeypots, and any contact with them triggers an inquiry. Installing a server with information marked "senior leaders' evaluations and important financial data" may draw insiders and hackers, but as soon as they access it, the Security Operation Centre (SOC) will be notified and will act immediately. Anyone may mimic several computers with different operating systems on their computer using virtual machines (VM), which are software-based computers. They may try hacking from one VM to another using this. Training may be carried out in virtual environments without the expense of travel. Second Life is a well-known virtual world with a commercial focus. utilize a live CD like Backtrack to boot your present computer into a Linux operating system so you can utilize some of the technologies we have been discussing.

Targeted Capabilities

The many systems, kinds of information, and businesses that the adversary is attempting to compromise are broken down into targeted capabilities. National Critical Infrastructure, Corporate, Personal, and Information Technology Infrastructure make up the main categories. It's common for critical infrastructure to include elements of the other categories. Typically, corporate information will have integrated personal and IT infrastructure [4].

National Critical Infrastructure Protection (CIP) Includes

Finance, law enforcement, the legal system, the military, the chemical and energy industries, the state, emergency services, plans, manufacturing, and aviation. There would be significant effects if even just one of them were unavailable. After the 9/11 attacks, there was a decline in confidence in aviation security, which had indirect economic effects. A bank run can result from people losing faith in the reliability of our financial institutions. There would be negative effects on the economy and public health if the electricity system were to fail. The problem is that private organizations that must weigh risk vs profit are in charge of managing the majority of this vital infrastructure. The competition is interested in corporate assets such as email accounts, confidential information, financial records, policies, proposals, and organizational choices. Depending on the information, nation governments, criminal gangs, hacktivists, and insiders may all be interested in various aspects of the business. For insurance companies, criminals, espionage targets, and your personal foes, personal information like health records and financial data (banking and credit card accounts) are high value targets. Finding out as much information as possible on a senior member of the US military today would be the first stage in any attack. The same can apply to law enforcement organizations that concentrate on the drug trade. More and more private information is being posted online by the generation of digital natives. All of this data relates to two key issues: fraudulence and social engineering [5].

Information Technology (IT) Infrastructure

Infrastructure related to information technology (IT) is a target for two reasons. In order to uncover weaknesses, hackers may wish to utilize the infrastructure for their own purposes, such as creating

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

a botnet, or they may just want to know what network devices and operating systems (Windows/OS X) are accessible. It may be possible to acquire insight into how to gain unauthorized access by mapping the Web sites or understanding their architecture.

The threats include the methodologies, tools, and strategies deployed by the various attacker types, as well as a review of the crucial components of the defensive architecture put in place to safeguard our systems and the broad categories of data the hackers are pursuing. Although each of them will be discussed in more depth in later chapters, this foundation is meant to serve as a unifying force. The purpose of Chapter 8 is to provide an overview of the issues in the cyber world. It separates the issues so that they may be compared to one another and makes it easier to have a conversation about setting priorities and allocating resources.

How one should defend oneself at home is the query that is asked the most after addressing these cyberthreats. "Safe behaviors" are the response. The fundamentals, like using a firewall, current antivirus software, updating all apps, storing sensitive and financial information on a portable hard drive that is only plugged in when needed, and backing up important data to a location that won't be destroyed in the event that the system is stolen or destroyed, go a long way. Basic security requires all of them, but they may all be circumvented by bad security habits like using weak passwords, visiting sites known to be malware hotspots, reading emails, or accepting invitations on social networking sites from people you don't know. Although "security through obscurity" does not exist, we should make an effort to avoid becoming the "low hanging fruit" that is readily PWNed [6], [7].

Cybersecurity Governance

It is important to build a cybersecurity governance and risk management program that is suitable for the organization's size. The owners and directors must see cybersecurity risk as a substantial business concern. With appropriate measurement criteria, outcomes should be tracked and managed on a par with regulatory, operational, financial, and reputational risks. The risk assessment and associated best practices may be taken into account via voluntary frameworks. The Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) contains five continuous and concurrent functions, for instance:

i. **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.
ii. **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
iii. **Detect:** Develop and implement appropriate activities to identity the occurrence of a cybersecurity event.
iv. **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
v. **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Protection from Malicious Software and External Attack

Every organization has to make sure it is prepared to handle a dynamic threat environment since new threats are always emerging. Some of the most important system tools and solutions that are used to lessen these hostile assaults include the following:

i. Hardware and software firewalls are used to safeguard a system against intrusion by users who connect to it via internal as well as external communication channels.
ii. Web proxy and malware/spyware security tools shield the computer from programs that may come via pop-up windows or have more sinister intentions, such recording user names and passwords for fraudulent usage.
iii. Anti-spam software guards against the clogging of email inboxes with unsolicited broadcast email.
iv. Anti-phishing software safeguards users accessing websites made to collect user information that may be used fraudulently in the future.

Any well-managed system using a defense in depth approach must have all of these. It is important to weigh the expense of defending against such risks against the potential costs of an attack, which might include data loss, fraud, and the cost of reconstructing systems. It is advised to work with a reliable, well-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

known source. Some businesses claim to provide these services, but the utilities themselves may include harmful malware. Use of free software or software from an unidentified provider should be avoided. Generally speaking, it is better to use the utilities advised by the company's systems integration technical support team, since they will be in charge of its installation, setup, and upkeep [8].

It's crucial to maintain these apps. Every day, new harmful software is created. The majority of software providers guarantee that their databases get at least a daily automated update to maintain the system's level of protection. It's crucial to make sure these updates are applied properly.

DISCUSSON

Hardware providers should establish maintenance agreements so that hardware issues may be immediately fixed. The service standards that the provider will satisfy in the case of failure should be specified in these contracts. Servers, switches, and backup technologies are examples of critical gear that needs immediate care. Many contracts provide for a four-hour reaction time in the event that these components fail. Individual workstations and other less important gear may have slower reaction times. Some businesses, especially those in distant locations, buy extra parts for crucial components that are more likely to fail, including power supplies, so they can swiftly replace a failing component. Businesses that depend on maintenance contracts should make sure the support firm has enough spare parts on hand to satisfy the organization's service level requirements. In order to guarantee that the systems are properly integrated and maintained, the caliber of the organization's external IT support business is essential. Concerns that must be taken into account while choosing a suitable firm include the following. their familiarity and expertise with the hardware and operating system setup of the company. their familiarity and proficiency with the application software used by the company. A guarantee of the competence of the individuals in the organization is provided by certifications held with key hardware and software firms. The number of employees in the business who possess the necessary expertise to support the system is crucial since relying too much on a single person might result in expensive delays and downtime if that person is absent for any reason. Their capability to provide support services remotely to allow quick resolution of problems at a fair price. To make sure the third party is delivering the services in accordance with the organization's expectations, proper due diligence and vendor risk management are required [9]–[11].

CONCLUSION

The spread of cyber weapons keeps pace with the continued expansion of interconnectivity. There are four things to note as a conclusion: First, the international rules-based system for cyberspace is still in its infancy; creative thinking is required to ensure that countries like Canada can take the lead in developing the governance architecture. Second, there is a high level of secrecy surrounding the development and use of cyber weapons; as a result, nations are unprepared for the magnitude of cyberattacks that are likely to occur, and it is not only state actors that are launching attacks. The public is now an increasing target for both criminal and state actors, ranging from ransomware attacks to data breaches to the spread of disinformation, so it is necessary to foster a culture of cybersecurity awareness to manage risks and improve cyber hygiene practices. Malicious attack techniques are sold online for a relatively low price, meaning that attack mechanisms can be bought and deployed by anyone.

REFERENCES

[1] V. Smyth, “Cyber-security fortresses built on quicksand,” Netw. Secur., 2015, doi: 10.1016/S1353-4858(15)30068-4.

[2] Z. Maqbool, P. Aggarwal, V. S. C. Pammi, and V. Dutt, “Cyber Security: Effects of Penalizing Defenders in Cyber-Security Games via Experimentation and Computational Modeling,” Front. Psychol., 2020, doi: 10.3389/fpsyg.2020.00011.

[3] H. Aldawood and G. Skinner, “An academic review of current industrial and commercial cyber security social engineering solutions,” in ACM International Conference Proceeding Series, 2019. doi: 10.1145/3309074.3309083.

[4] M. Rizal and Y. Yani, “Cybersecurity Policy and Its Implementation in Indonesia,” JAS (Journal ASEAN Stud., 2016, doi: 10.21512/jas.v4i1.967.

[5] M. Dawson, R. Bacius, L. B. Gouveia, and A. Vassilakos, “Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors,” L. Forces Acad. Rev., 2021, doi: 10.2478/raft-2021-0011.

[6] J. O. Oyelami and A. M. Kassim, “Cyber security defence policies: A proposed guidelines for

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

organisations cyber security practices," Int. J. Adv. Comput. Sci. Appl., 2020, doi: 10.14569/IJACSA.2020.0110817.

[7] D. Preuveneers and W. Joosen, "Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence," J. Cybersecurity Priv., 2021, doi: 10.3390/jcp1010008.

[8] P. Zave and J. Rexford, "Patterns and Interactions in Network Security," ACM Comput. Surv., 2021, doi: 10.1145/3417988.

[9] NATO, "NATO Cyber Defence," NATO Factsheet, 2019.

[10] G. Kumar and K. Kumar, "Network security – An updated perspective," Syst. Sci. Control Eng., 2014, doi: 10.1080/21642583.2014.895969.

[11] P. Lupien, G. Chiriboga, and S. Machaca, "Indigenous movements, ICTs and the state in Latin America," J. Inf. Technol. Polit., 2021, doi: 10.1080/19331681.2021.1887039.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Analysis of Computer Controlled Infrastructure for Cyber Security

Dr. Ramadass Mahalakshmi
Associate Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India
Email Id-mahalakshmi@presidencyuniversity.in

Abstract: ***Computers control our power grids, roads, public transportation, telecommunications and more. Malicious attacks from either foreign or domestic sources can paralyze key services and communications. With the rapid proliferation of the Internet of Things (IoT) within critical infrastructure and growing evidence of state-sponsored cyber-attacks, both government agencies and private-sector organizations have increasing concerns about cyber security threats that directly impact critical infrastructure. Understanding the types of cyber threats and how cyber security professionals can respond to them is an important step toward minimizing threats. Cyber security professionals may work with privately-owned companies or public agencies.***

Keywords: ***Cyber Security, Cyber Attack, Computer System, Cyberoam, Internet of Thing***

INTRODUCTION

Next is the physical infrastructure, this includes power, backup generators, Heating Ventilating and Air Conditioning (HVAC), surge control systems, connectivity (cabling), hardware, software, and people. The physical systems are vulnerable to surveillance, vandalism, sabotage, and attack. Much of this infrastructure is controlled by Industrial Control Systems (ICS) or as they are more commonly known Supervisory Control and Data Acquisition (SCADA) programs which are vulnerable to hacking or denial of service attacks. Note that SCADA is a subset of ICS but has become synonymous in the media. This list does not address the potential environmental disaster factors. If the threat cannot conduct a kinetic attack or hack the system then there is always the wetware vector. It is often easier to attack users than it is the equipment. So when attacking the physical there are a number of options to create the desired impact [1].

Organizational View

Organizations can be divided into commercial including critical infrastructure and government generally divided into federal agencies and the military. These different organizations all approach cybersecurity differently. Most commercial companies are market driven and try to spend just enough on security to manage risk appropriately. These companies must make decisions based on Return on Investment (ROI) which leads to the eternal struggle between the Chief Financial Officer (CFO) and the Chief Information Officer (CIO). Today many CIOs calculate Return on Security Investment using formulas like Annualized Loss Expectancy (Vulnerability × Threat × Asset Value = Total Risk then Total Risk × Countermeasures = Residual Risk). This would go something like: chance of getting a virus attack is 100% in fact expect one a day, cost is 3 h of lost productivity and 1 h of IT support times total number of employees = 365 viruses × $450 labor × 200 people = $3,285,000 or buy antivirus for $40 per system for total of $8000 and reduce risk to acceptable level. With the need for cost saving in the government these types or calculations are becoming more common in the military today.

The DOD has a very hierarchical authority structure but it is not simple. Despite standing up CYBERCOM, the individual services (Army, Air Force, Navy/Marines) still have the authority and budget to decide how to implement cybersecurity. Each branch of the service has a name for their portion of the network. Defense Information Systems Agency (DISA) runs the Global Information Grid (GIG), Air Force has C2 Constellation, the Army has LandWarNet, and Navy has FORCEnet.

There are also different levels of classification on information and networks. The DOD uses

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Unclassified, For Official Use Only (FOUO), Secret, Top Secret, and Special Access Program/Special Access Required (SAP/SAR). The associated networks are Non-Secure Internet Protocol Router (NIPR) for unclassified, Secure Internet Protocol Router (SIPR) for secret, and Joint Worldwide Intelligence Communications System (JWICS) for Top Secret. In addition, there are separate networks like the Defense Research and Engineering Network (DREN) for research. Finally, deployed forces build their own networks in theater that connect too many of these "reach back" networks as well as must connect to fellow coalition nations via multi-national forces networks. An example would be a unit from Fort Carson deployed to Afghanistan that would have to build a network in country or theater, would want to connect back to resources at Fort Carson, and connect to other international forces they are teamed with. It is not unusual to see a Tactical Operation Center (TOC) with 6–12 terminals representing the different networks. It is easy to see that there is not a clear chain of command for the network of networks supporting DOD.

As important as these networks are they don't include the full scope of the modern virtual battlefield. Today command and control of forces is done digitally, weapon systems are connected to the network and depend heavily on computing power, intelligence dominance is key to our ability to win on the modern battlefield and it is completely dependent on computer applications. During one military simulation a young Airman was asked what would happen if the network went down, he said they would have to stop flying. That is of course untrue as leaders of the pre-digital generation were flying similar missions long before computers were used for command and control but the generation perception and dependence on the network was startling. Note that the loss of the TOC network would have a huge impact on the ability to process orders nearly as fast or accurately as the current "information dominance" systems allow [2], [3].

When we talk about CYBERCOM and the Services (Army, Navy, Air Force) it is important to remember that the Services train and equip the forces and the Combatant Commanders call on the services to provide forces for their missions. Strategic Command (STRATCOM) has the mission to "ensure US freedom of action in space and cyberspace". Next is Cyber Command (CYBERCOM) whose mission is to "plan, coordinate, integrate, synchronize, and conduct activities to: direct the operations and defense of specified Department of Defense information networks and, prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries". Each Service has a Cyber unit that supports CYBERCOM, the Air Force has the "24th Number Air Force," the Army has "Army Cyber," the Navy has the "10th Fleet" and the Marines have "Marine Forces Cyber." Closely aligned to these forces is the Intelligence Community—specifically the National Security Agency (NSA). This results in different priorities based on the different mission each organization has.

It is important to note that there are US Codes that set the rules for how these units operate. There are a number of titles that provide specific guidance. Title 10 is Armed Forces and is the law that regulates how war is fought. Title 50 is War and National Defense and generally covers intelligence and counter intelligence. It is interesting to note that some units had their authorized mission changed from being under Title 50 to Title 10 as part of the CYBERCOM stand up. Title 18 is Crimes and Criminal Procedure which covers taking the attacking party to court. Many people are now talking about the need to integrate these three into one integrated process (sometimes called Title 78). Other titles that often used are Title 32 which is National Guard and Title 14 which is the Coast Guard. These forces are not as restricted by laws like Posse Comitatus which restricts the federal government use of the military for law enforcement. Today we see Joint Operation Centers with forces from multiple "title sources" or "forces" to allow them to operate effectively based on the different rules they must comply with.

Cyber Fits in the War-Fighting Domains

Historically there were only two war-fighting domains, land and sea. Land is simply the area where combatants fought. Over time there were developments in weapons that would give one side or the other an advantage but they would face each other on the field-of-battle. Then the sea became both a separate war-fighting domain and a part of the land domain. The Maritime domain includes the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. The littorals have two operational environments: Seaward, the area from the open ocean to the shore, which must

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

be controlled to support operations ashore and Landward, the area inland from the shore that can be supported and defended directly from the sea. Ships would fight battles to both control the sea and support land battles. As technology continued to influence the battlefield, airplanes were introduced. The air domain is the atmosphere, beginning at the Earth's surface and extending to the altitude where its effects upon operations become negligible. The first airplanes were used for reconnaissance but were soon armed and fought both air to air and air to ground engagements. Then warfare reached space. Space is the environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere. This was a unique domain as it was used by the other domains rather than a domain where combat was fought (though at some point it will become another battlefront). Finally, cyberspace became so vital to the war-fighters it was declared a domain. It is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Modern commanders depend on it and are actively studying how to fight and win the next war on it [4], [5].

i. Land

As we look back at the progression of warfare on land, we see there have been many Revolutions of Military Affairs (RMA). The rock gave way to the club, which was beat out by the spear and then the bow. Horse-mounted soldiers had an advantage over ground troops and then the stirrup gave them a tremendous advantage. Guns and artillery increased the rate at which armies could kill each other as well as the effective range at which they could kill. Then came the tank and machinegun. Each of these RMA changed how armies fought. New doctrine, tactics, and organizational structures had to be developed. Should we integrate the new weapons into every unit or build a unit of pure machineguns/tanks? The decision was tank units should consist on tanks by themselves but the machinegun should be integrated into every unit. The decision to make tank units of pure tanks has been reversed. Today, the tank is normally integrated with infantry to form "combined arms task forces" so the commander can leverage each unit's strengths. These historical lessons in transformation must be studied to find how to most efficiently develop methods of fighting in cyberspace.

ii. Sea

In many ways the sea is an analogous battlefield to cyberspace. Like cyberspace it is a large area where ships can easily move without detection so the defender has the challenge of detecting where the threat is. No one side can control it. The criminal elements operating on the Internet are comparable to the pirates of old who would interdict and influence the lines of commerce. There were eventually international agreements developed to deal with these threats. Another example we can draw from the Navy is the development of the Flattop or Aircraft Carrier. For years the battleship was the measure of a nation's sea power but the introduction of the Flattop caused a paradigm shift and soon strategies, doctrine, and tactics were built around it. Most senior officers had built their careers around the battleship and the defense industrial base was heavily investing in the battleship so they strongly resisted the transformation. They refused to see the need to change based on a new capability. This cultural blindness is impacting the transformation to computer network operations in many of today's organizations. At the tactical level many security professionals still base their strategies on outdated technologies, even though the industry and the battlespace have transformed, and evolved. They are still focused on perimeter defenses and ignore the mobile devices being used by their work force. At the senior leadership level, the lack of understanding of the technology and its implications in some organizations are impeding the development of doctrine to fight the next war [6].

iii. Air

Airpower is similar to cyber power because it is a domain dominated by technological advancements. Early on there were major leaders developing strategies, doctrine, and tactics. General Giulio Douhet was an Italian officer who was one of the first real theorists supporting the use of Air Power. He felt that there was no defense against bombers, it would terrorize populations into surrender, and he advocated the use of explosive, incendiary, and poison gas bombs against population centers as everyone contributes to the total war effort so everyone is legitimate target. General Douhet was court-martialed for his outspoken

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

beliefs.

iv. Space

Space is very comparable to cyberspace in that it is generally considered to be an enabler to the other domains. It provides communications paths for most long-haul communications systems, Command and Control (C2), Intelligence Surveillance and Reconnaissance (ISR), navigation based on Global Positioning System (GPS), phones-radios-television-financial transactions, and surveillance for wide area reconnaissance- weather-mapping and commercial imaging (i.e. Google maps). The George C. Marshall Institute produced a great series called "A Day without Space" which lays out all the impacts. Space provides some great examples on how to integrate a new technology into the armed forces. Space started as a military dominated domain that has transitioned to a commercial market just like cyber operations. It is a technology that integrated into the other domains to the point they are dependent on it. It is an area that requires unique skills so the management of the work force presents a challenge. It takes time to build senior leaders for a new technology and as the commercial demand takes off the competition for the workforce gets fierce. It is very hard to retain skilled operators in cyberspace related fields.

v. Cyber Domain

Cyber is ubiquitous in all the other modern domains. "I think that a day without cyber brings you back to about World War I days," said Lt. Gen. William T. Lord, Air Force chief of war-fighting information. When we talk about the cyber domain some will say it is limited to the hardware that runs the military networks (computers, routers, firewalls), others will say it is the military networks and the supporting infrastructure (i.e. defense contractors and long haul communications providers), a few believe it is all government systems, still others feel it is all systems connected to the Internet all private and governments systems. As we look for precedents, we can see Maritime law could be used, or international space treaties could apply or maybe we could develop a cyber-manifest destiny. Some of the answers are overly simple or fit within current legal rules but ignore the reality of how interconnected these systems are. The problem is complex and, much like defining the boundaries in an insurgency conflict, may require different answers for different audiences. This domain is in need of theorists, strategies, doctrine, and tactics that shape what the domain and cyber war itself is scoped to include and exclude.

Others would say Korea and Vietnam were wars but the counter is that technically they were police actions. If Korea was a war then we are still at war with North Korea. Many presidents have openly talked about the Cold War but a "war" was never declared. The US declared a "War on Drugs" and "War on Terrorism" but again it was not a war against another country but rather on a problem that had reached the level it was a national security issue, if this is the standard we measure by then we could have a pure cyber war. The US has been in multiple wars in the Middle East (Iraq twice and Afghanistan) but these were not formally declared "wars," some would say they are part of the "War on Terrorism." Still others will talk about economic warfare. The last time America was in a formal war was World War II, the concept of what a war means is changing. These have been very traditional wars and if they are the standards, we measure a "war" by then there is no such thing as cyber war. Today the Internet is very similar to how the Wild West is portrayed in movies. Over the course of a movie they might have to deal with Indian attacks, Mexican banditos, and bad weather, criminals from our own community and Mexican Army invasions. Indian attacks are a form of guerilla warfare, banditos are non-state actors but may have informal support from their host nation, weather equates to the environmental impacts that create noise in the system making things unpredictable, criminal acts if they get bad enough may become a threat to the community and may require the aid of the state or federal government to solve and military invasion is a full scope war which could require the full weight of the country to address. Any of these can wipe us out and may need to be addressed by the local sheriff, the rangers or the US Army depending on how the politicians choose to react. So, the question of if we are in a cyber war today is answered by the simple statement "don't care what we call it just get us some help!"[7], [8]

DISCUSSION

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Hardware providers should establish maintenance agreements so that hardware issues may be immediately fixed. The service standards that the provider will satisfy in the case of failure should be specified in these contracts. Servers, switches, and backup technologies are examples of critical gear that needs immediate care. Many contracts provide for a four-hour reaction time in the event that these components fail. Individual workstations and other less important gear may have slower reaction times. Some businesses, especially those in distant locations, buy extra parts for crucial components that are more likely to fail, including power supplies, so they can swiftly replace a failing component. Businesses that depend on maintenance contracts should make sure the support firm has enough spare parts on hand to satisfy the organization's service level requirements. In order to guarantee that the systems are properly integrated and maintained, the caliber of the organization's external IT support business is essential. Concerns that must be taken into account while choosing a suitable firm include the following. their familiarity and expertise with the hardware and operating system setup of the company. their familiarity and proficiency with the application software used by the company. A guarantee of the competence of the individuals in the organization is provided by certifications held with key hardware and software firms. The number of employees in the business who possess the necessary expertise to support the system is crucial since relying too much on a single person might result in expensive delays and downtime if that person is absent for any reason. Their capability to provide support services remotely to allow quick resolution of problems at a fair price. To make sure the third party is delivering the services in accordance with the organization's expectations, proper due diligence and vendor risk management are required [9]–[11].

CONCLUSION

The spread of cyber weapons keeps pace with the continued expansion of interconnectivity. There are four things to note as a conclusion: First, the international rules-based system for cyberspace is still in its infancy; creative thinking is required to ensure that countries like Canada can take the lead in developing the governance architecture. Second, there is a high level of secrecy surrounding the development and use of cyber weapons; as a result, nations are unprepared for the magnitude of cyberattacks that are likely to occur, and it is not only state actors that are launching attacks. The public is now an increasing target for both criminal and state actors, ranging from ransomware attacks to data breaches to the spread of disinformation, so it is necessary to foster a culture of cybersecurity awareness to manage risks and improve cyber hygiene practices. Malicious attack techniques are sold online for a relatively low price, meaning that attack mechanisms can be bought and deployed by anyone.

REFERENCES

[1] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informatics*, 2013, doi: 10.1109/TII.2012.2198666.

[2] G. Hatzivasilis *et al.*, "WARDOG: Awareness Detection Watchdog for Botnet Infection on the Host Device," *IEEE Trans. Sustain. Comput.*, 2021, doi: 10.1109/TSUSC.2019.2914917.

[3] HM Government, "Cyber Essentials Scheme: Assurance Framework," *Comput. Secur.*, 2014.

[4] HMG, "Cyber Essentials Scheme Requirements for basic tecnical protection from cyber attacks," *Comput. Secur.*, 2014.

[5] P. A. S. Ralston *et al.*, "Cyber Essentials Scheme," *Comput. Secur.*, 2014, doi: 10.1109/INDIN.2013.6622963.

[6] R. G. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva, and C. Forsythe, "Log Analysis of Cyber Security Training Exercises," *Procedia Manuf.*, 2015, doi: 10.1016/j.promfg.2015.07.523.

[7] HM Government, "Cyber Essentials Scheme Summary," *Comput. Secur.*, 2014.

[8] D. Seo, Y. I. You, and K. Lee, "Security control analysis of ICS," *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.3.15.

[9] R. Gupta, R. Agarwal, and S. Goyal, "A Review of Cyber Security Techniques for Critical Infrastructure Protection," *Int. J. Comput. Sci. Eng. Technol.*, 2014.

[10] UKGovt-NCSC, "Cyber Essentials Scheme - Requirements," *Comput. Secur.*, 2014.

[11] H. Yang, "Delay Performance and Cybersecurity of Smart Grid Infrastructure," *ProQuest Diss. Theses*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Introduction to Cyber Doctrine

Mr. Mrutyunjaya Mathad
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India
Email Id-mrutyunjaya@presidencyuniversity.in

Abstract: ***The defensive cyber doctrine includes measures for preventing, foreseeing, detecting, and guarding against cyberattacks. The doctrine's application is restricted to defensive and non-military responses to and identification of the source of the assault. The policy explains how defense will deal with online dangers and make sure that its tools are safe from intruders' assaults. The foundations for maintaining a strong cyber security posture in a changing strategic environment are presented, along with the road to a cyber-resilient defense. The circumstance when an action occurs outside of a nation's boundaries but has its greatest impact there gives that country jurisdiction since it falls under the "effects" theory. Consider the scenario when a Pakistani fires over the border, injuring an Indian.***

Keywords: Cyber Crime, Cyber Doctrine, Cyber Security, Data Integrity, Information Technology.

INTRODUCTION

The guiding concept used by the armed forces or subsets thereof to direct their operations in support of governmental goals is known as doctrine. Although authoritative, its use calls for discretion. Military strategies were developed based on it. It directs tactics, techniques, and procedures (TTPs) and is influenced by tradition. We will discuss the doctrine that already exists, the doctrine that needs to be transferred to the cyberspace, the related non-military agencies' advice, and lastly the exercises that are being carried out to build doctrine.

Current US Doctrine

As of right now, cyberwarfare is not defined by the US military. Computer security, Information Security (InfoSec), Net Centric Warfare, Information Assurance (IA), Information Warfare, Cybersecurity, and finally Cyber Warfare have all been terms used to describe this capacity throughout time. Nowadays, when military strategists employ the phrase "cyber," they also incorporate offensive capabilities. Previously, these concepts were only concerned with defense. Computer network operations (CNO) are the most often used definition of cyber. Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND) are the three tasks that fall under CNO [1].

Information Operations (IO), which includes CNO, contains a number of fundamental, supporting, and associated capabilities that are shown in detail in Figure 1. Information assurance (IA) and CNO are two fields that overlap. While IA is described as measures that safeguard information and information systems' availability, integrity, authentication, secrecy, and non-repudiation, CNO is defined by the three aforementioned functions. By including protection, detection, and response capabilities, this also involves offering for the restoration of information systems. Consequently, we might conceive of IA as creating and maintaining networks while CNO plans and engages in combat over them, similar to the distinction between maintaining the Tanks in an Armour Battalion and employing them to engage in combat.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

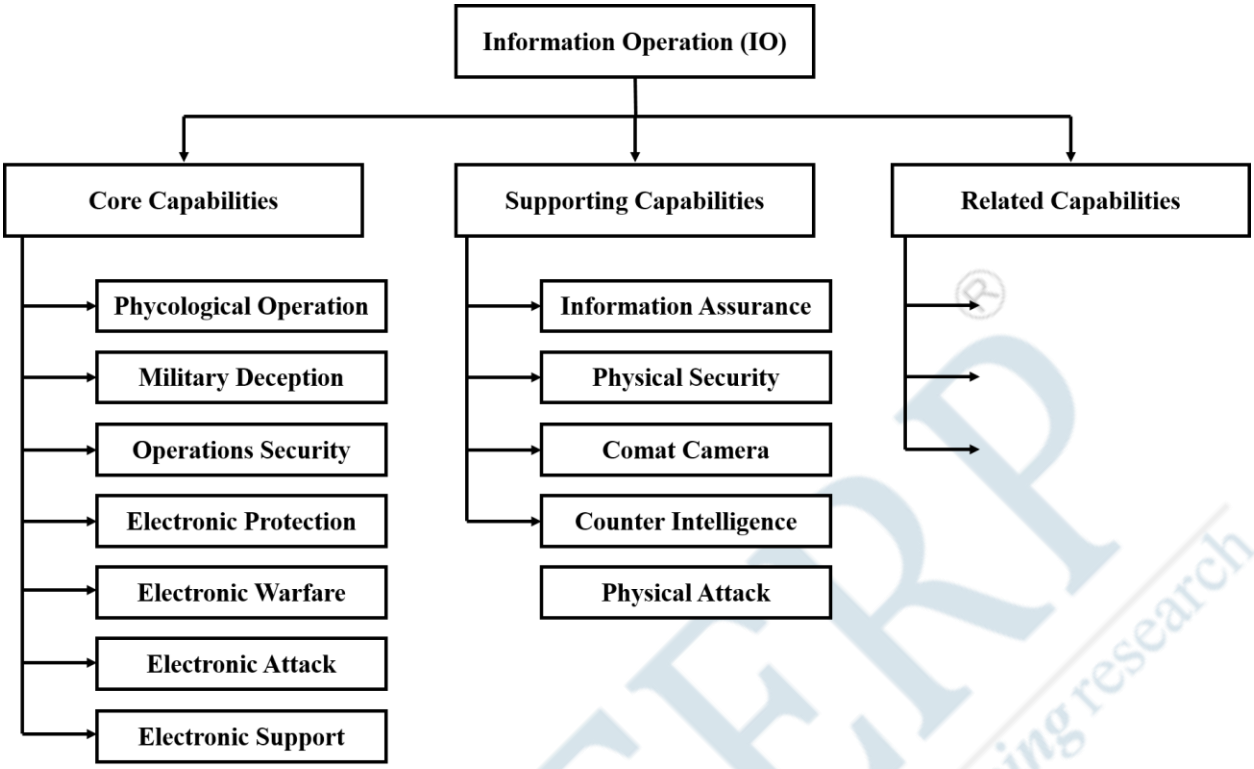

Figure 1: Illustrated the Information Operations Framework

Information Operations Framework

The manner in which cyber doctrine is being created at the moment raises certain questions. In 2006, the primary Joint Publication on cyber doctrine was released. Since doctrine is not often updated, there is fear that it may rapidly become obsolete in a world where Moore's Law is in effect and capabilities double every 18 months. The fact that the services do not use the same terminology the Army and the Air Force have distinct definitions of information operations—is another possible problem. Another difficulty is that much of the ideology is classified, which causes various organizations to have access to different information and base their choices only on that knowledge. Last but not least, there is the issue of fundamental mindset regarding the significance of cyberwarfare as a component of combat operations. Some leaders believe that cyberspace is only a supporting function for administrative activities, while others feel that cyberspace is embedded in everything from today's command and control systems to the weapons systems and it is the critical centre of gravity for the nation [2].

US Forces

In May 2011, the White House unveiled its International Cyberspace Strategy, which put a strong emphasis on prosperity, security, and openness in a networked world. "The United States will pursue a global cyberspace strategy that supports the innovation that propels our economy and enhances both local and global quality of life. We base all of our work on concepts that are crucial to the future of the Internet as well as American foreign policy. Put privacy and information freedom front and center. It had a broad aim and specific goals:

i. **Goal:** The United States will collaborate with other nations to advance an information and communications network that is open, interoperable, secure, and dependable, supports global trade and commerce, bolsters global security, and promotes innovation. We shall create and maintain an environment where responsible behavior standards serve as a guide for governments' activities, foster collaborations, and uphold the rule of law in cyberspace in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

order to accomplish that aim.

ii. **Diplomatic Objective:** The United States will seek to forge incentives and foster consensus in an effort to foster international cooperation and responsible stakeholder behavior among nations that recognize the fundamental benefit of an open, interoperable, secure, and reliable cyberspace.

iii. **Defense Objective:** In cooperation with other countries, the United States will promote responsible conduct and oppose those who attempt to disrupt networks and systems, discouraging and deterring hostile actors while maintaining the right to protect these crucial national assets as necessary and appropriate.

Department of Defense Strategy for Operating in Cyberspace was released in July 2011 and has fire initiatives:

1. **Strategic Initiative 1:** Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
2. **Strategic Initiative 2:** Employ new defense operating concepts to protect DoD networks and systems.
3. **Strategic Initiative 3:** Partner with other US government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
4. **Strategic Initiative 4:** Build robust relationships with US allies and international partners to strengthen collective cybersecurity.
5. **Strategic Initiative 5:** Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Cyberspace activities are under the control of US CYBERCOM. The new command was formed by the US Secretary of Defense in a letter that was signed on June 23, 2009. Its first Commander, Gen. Keith Alexander, recently told Congress in a statement that "the Department of Defense networks that we defend are probed roughly 250,000 times an hour." Another example is when the Department discovered in 2006 that 10–20 gigabytes of data had been remotely stolen from NIPRNet. Then he cited Deputy Secretary William Lynn as saying that Cyber Command's "linking of intelligence, offence, and defense under one roof" as its primary strength. To do this, the National Security Agency (NSA) provides crucial knowledge. US Cyber Command has three primary operational axes, according to Gen. Alexander. In order to enable the Department of Defense to carry out its duties, we oversee the Global Information Grid's operations and defence. We also remain ready to protect the freedom of action of our country in cyberspace.

The Department's cyberspace policy will be guided by five principles: Leverage US technology advantages, make our defences active, protect our essential infrastructure, and remember that cyberspace is a defensive environment. How much importance the leadership is focusing on this new area of warfare may be seen by the focus on elevating cyber doctrine and policy to the highest level of military command. They have had to reallocate finances since there is not much money to make this happen until the new command catches up with the DoD Programme Objective Memorandum (POM) spending cycle, but they are nevertheless making it happen now because they believe it is crucial to the military's future success. Figure 3.2 illustrates the considerable number of cyber centres that the US government needs to coordinate. Many think Cybercommute is best suited to do this task, however according to doctrine, Department of Homeland Security should be in charge of it.

Cyber Centers

The Honorable W. has commenced this command. "Mac" Thornberry, the chairman of the House of Representatives' Subcommittee on Emerging Threats and Capabilities Committee on Armed Services, has criticized the DOD for not yet having an overall budget estimate for cyberspace operations that cover computer network attack, computer network exploitation, and classified funding. In February and March 2011, the Department of defense (DOD) sent Congress three distinct budget projections for its cybersecurity initiatives for fiscal year 2012 ($2.3 billion, $2.8 billion, and $3.2 billion, respectively). The three budget views primarily concern the Defense-wide Information Assurance Program and do not account for all full-spectrum cyber operation costs, such as those associated with computer network exploitation and computer network attack, which are covered by classified programs funded by the national intelligence and military intelligence program budgets [3], [4].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

US Air Force

Major General Richard E. Webber, the first US Air Force commander of the 24th AF, informed lawmakers that creating and enhancing cyberspace situational awareness is the 24th AF's top priority. Additionally, a Cyber Operations Liaison Element (COLE) has been created to serve as liaison officers (LNO) and assist the necessary knowledge transfer between mission planners and cyber planners. The Air Force has put the most effort into integrating cyber operations into its units at this time. They were the first to take action to establish a cyber-command, and they have actively attempted to translate the lessons learnt from creating organizational structure and doctrine for space to cyberspace.

The Judge Advocate General will "ensure that all weapons being developed, bought, built, modified, or otherwise being acquired by the Air Force that are not within a Special Access Program are reviewed for legality under Law of Armed Conflict (LOAC), domestic law, and international law prior to their possible acquisition for use in conflict," according to Air Force Instruction 51-402, which was published by the Air Force on July 27, 2011.

US Navy

The US Navy is taking steps to improve its cyber capabilities. Lieutenant-Admiral David J. The US Navy is prominent and dominant in the fields of ISR, cyber warfare, C2, and information and knowledge management, and as information becomes a Main Battery of US Navy capability, warfighting wholeness will replace today's subpar stovepipes, according to "Jack" Dorsett, the Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI). In order to create a fully-integrated Intel, C2, Cyber, and Networks capability, the Navy will transition from platform-centric to information-centric procedures. The last set of principles they will concentrate on are: Every platform is a sensor, every sensor is networked, Build a little; test a lot, Spiral acquisition, Plug-n-play sensor payloads, Reduce afloat/airborne manning, Transition to remoted, automated, One operator controls multiple platforms, and Emphasis UAS and autonomous platforms. This set of objectives is based on the Navy's ambition to deploy resources more quickly and affordably. In order to cope with the new submarine threat, the Navy turned to its past and intended to apply the lessons it had learned from setting up the 10th fleet during World War II. It also wanted to concentrate on how new technology was affecting the battlespace. They have taken several difficult decisions, such as merging the N2 (Intelligence) and N6 (Communications/Networks) staff roles under the Information Dominance directorate in order to boost personnel efficiency and integration. These modifications demonstrate how seriously and urgently the prospect for cyberwarfare is being taken; they do not want to be seen preparing for the final conflict.

US Army

Today, the US Army is officially addressing the creation of its cyber doctrine. In January of this year, the US Army Training and Doctrine Command (TRADOC) released a Cyberspace Operations (CO) Concept Capabilities Plan (CCP), which outlines the framework under which the Army expects to conduct cyber operations in the timeframe 2016–2028. TRADOC has coordinated concept development for cyber warfare with stakeholders across the Army. In the present operational context, they are concentrating on three aspects of cyber: the psychological conflict of wills, strategic engagement, and the cyber-electromagnetic contest. In the cyber-electromagnetic competition, Cybercops refers to the strategies used to achieve an edge, safeguard that advantage, and disadvantage opponents. CyberOps are common military engagement actions that are focused on winning the cyber-electromagnetic competition rather than being an end in and of themselves. They are a crucial component of Fire Support Operations. CyberOps are ongoing; everyday battles take place, often without the deployment of extra personnel. As a result, the architecture created for Army Operations provides four components for CyberOps: cyber warfare (Cyberwar), cyber network operations (CyNetOps), cyber support (CyberSpt), and cyber situational awareness (CyberSA). For more information on how these components connect to one another, see Figure 3.3. The Army is the only branch of the military that enjoys writing doctrine. They want it to be taught in their classrooms (at all levels) as a method to introduce new doctrine to the battlefield. The Army seeks to reeducate their force to comprehend the new environment, which is a distinct strategy from the other services that are focused on reorganization [5], [6].

CyNetOps Framework

Additionally, the Army is leaving the classroom. The Army aspires to be able to use a new arsenal of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

cyberwarfare weapons and engage in combat in cyberspace. Army Cyber Command/Second Army commander Lt. Gen. Rhett Hernandez said that the strategy is to acquire both defensive and offensive capabilities, including instruments to do network damage assessments and make sure that no collateral damage is done to non-military organisations. He said on November 8 at the Milcom conference in Baltimore, Maryland, that field commanders should have a "full range of cyberspace capabilities" at their disposal, including the capacity to "seize, retain, and exploit" enemy networks. In the internet realm, the Army "seeks the same level of freedom to operate as we have in the land domain," he added. The command is still developing; it went into service in October 2010. The first-of-its-kind specialised computer network security brigade of the US Army is currently operational and has been sent to the front lines to assist combat-active troops. Till the teams are completely operational in 2015, the 780th Military Intelligence Brigade, which was first proposed in 2008, will be used in a restricted capacity. "We have a cyber expeditionary capacity to support Army troops in network defense. Currently, a team from our organization is deployed forward in Afghanistan. They go ahead to assist the brigade combat team in securing their networks, according to Col. John Sweet, commander of the brigade. Senior military commanders' commitment to working at the pace required to develop and deploy cyber warfare weapons is shown by the organizational adjustments they have made inside the regular planning cycle [7].

DISCUSSION

The Information Operations Condition (INFOCON) system procedures are the last aspect of contemporary US military doctrine that we shall discuss. This directive applies to all DoD systems and specifies the defensive posture that military networks must adopt in the event of an attack. When under increasingly intense assaults, the INFOCON goes from 5 to 1. This is the constant state of readiness for information systems and networks, often known as "routine" network operations (NetOps). A snapshot of each server and workstation in a typical functioning state will be created and maintained by system and network administrators. The typical operating baseline that may be compared to future alterations to spot unauthorized activity is established by this snapshot. To compare the known good picture of an information network with the actual state and spot unauthorized modifications, system and network managers will build an operational rhythm. User profiles and accounts are also examined, and checks are made for inactive accounts. By regularly validating the information network and its accompanying configuration, system and network managers will advance NetOps readiness. The effect on end users should be minimal. System and network administrators will check NetOps readiness for the information network more often. With proper planning and training, the impact on end users might be minimal for just a brief period of time [8]–[10].

CONCLUSION

The greatest level of NetOps preparedness is at this point. This condition deals with intrusion methods that are unable to detect or counter at lower readiness levels. System and Network Administrators may update the operating system software on important infrastructure servers during INFOCON 1 from a precise baseline. INFOCON 1 would end after baseline comparisons stopped showing unusual activity. End-user effects could be severe for a short while, but they can be reduced by planning and training. TROs are extra steps taken in response to certain incursion characteristics. They complement the existing INFOCON preparedness level and are specifically targeted. To provide a shared understanding of the degree of preparedness and mission effect of each extra INFOCON measure, TROs will detail all of the measures in standard language. The feasibility of the present IT staffs to carry out this demanding timetable is questioned since these INFOCONs are not routinely used. The good news is that these response criteria are significantly better than the previous set, which caused organizations to disconnect during an attack, resulting in a self-denial of service. Any local commander may raise the INFOCON level, but they are not permitted to reduce the degree of protection to that of the command above them. Last but not least, a TRO is a distinct response to a particular danger; the most recent example is the response against malware on thumb drives. The DOD banned the use of thumb drives after determining that the possibility of network compromise outweighed the operational implications of losing the capability.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

REFERENCES

[1] S. N. Romaniuk and M. Manjikian, *Routledge companion to global cyber-security strategy*. 2021. doi: 10.4324/9780429399718.

[2] D. De Santo, C. S. Malavenda, S. P. Romano, and C. Vecchio, "Exploiting the MIL-STD-1553 avionic data bus with an active cyber device," *Comput. Secur.*, 2021, doi: 10.1016/j.cose.2020.102097.

[3] A. Edegbeme-Beláz and D. Berzsenyi, *Hungary: from the groundworks to an evolving cyber security landscape*. 2021.

[4] S. Winterfeld and J. Andress, *The Basics of Cyber Warfare*. 2013. doi: 10.1016/C2012-0-02436-2.

[5] P. Zhesterov, "From visible pasts to an invisible presence: New criminological reality after planetary cyber attack 12/05/17 Wannacry," *Prz. Wschod.*, 2018, doi: 10.31648/pw.3002.

[6] T. H. Huh, S. Lee, and W. Y. Chang, "Strategy: Korea's Military Cyber Security Issues and Tasks," *Int. Area Stud. Rev.*, 2007, doi: 10.1177/223386590701000112.

[7] M. Canan and A. Sousa-Poza, "Complex Adaptive Behavior: Pragmatic Idealism," in *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.09.295.

[8] A. Zotti, "Global Change, Peace & Security: formerly Pacifica Review: Peace, Security & Global Change Inside cyber warfare," *Peace Secur.*, 2010.

[9] T. I. Faith, "American Biodefense: How Dangerous Ideas about Biological Weapons Shape National Security by Frank L. Smith III," *Technol. Cult.*, 2016, doi: 10.1353/tech.2016.0053.

[10] E. Park, "Objects, Places and Cyber-Spaces Post-Carpenter: Extending The Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA," *Yale J. Law Technol.*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Doctrine and its Strategy from Around the World

Mr. Murthy Hanumantharaya Ramesh
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-murthydhr@presidencyuniversity.in

Abstract: ***The defensive cyber doctrine entails the prevention, anticipation and detection of and protection against cyber-attacks. The scope of the doctrine is limited to reacting to and attributing the attack limited to defensive and nonmilitary measures. Commonly known as the 'effects' doctrine is the situation, where the action takes place outside the territory of a country, but the primary effect of that activity is within the said country, it assumed jurisdiction. For instance, a person from Pakistan shoots across the border and an Indian is injured in the process.***

Keywords: ***Antivirus, Cyberspace, Cyber Warfare, Cyber Security, Doctrine***

INTRODUCTION

We'll now go through some of the cyber doctrine and tactics that other countries are currently developing. We'll start with China and a few other significant Asian nations. Then discuss the nations of Europe. Despite being a significant role, Russia has a greater influence on crime than on combat, thus they won't be singled out specifically. We will examine potential private or mercenary organizations last. Military doctrine has a rich historical heritage, albeit it may not be as ancient as war itself. It is one of the five 'basic components' of battle, along with moral influence, weather, geography, and command, according to Sun Tzu's classic treatise The Art of battle, which was presumably composed in the fourth century BC. The recognition and study of tactics as a branch of warfare and the establishment of military academies to provide prospective officers with a formal education that would prepare them for their profession are two significant innovations from late eighteenth-century Europe that may be traced as the origins of military doctrine.

The interest in it has grown since the end of the nineteenth century, when the militaries of all the great nations began to devote a lot of time and effort to it. Military history has historically focused on the development of military doctrine. Our knowledge of the origins and characteristics of doctrine has grown along with the viewpoints on military history. Doctrine is the result of a difficult process in which a variety of factors come together to create a "standard operating procedure." There are various uses for doctrine. Its primary role is to provide a balanced interpretation of experience and to establish beliefs. The transmission of these ideas to successive generations is its second purpose. Its third purpose is to provide a shared foundation of knowledge and understanding that may serve as direction for action. The link between ideology and strategic choices is where all three of these roles are realized [1], [2].

Divergences in practice exist between France, the UK, and the United States on peace support operations and general emergency response to complicated situations for a variety of reasons. In cases when the goal is to reassure and protect third parties as well as to discourage possible aggressors, the United States places a greater priority on force protection and is less likely to put its personnel in danger. The US Army's much-touted "warrior ethos" is particularly at odds with the British Army's practical approach, developed over decades or perhaps centuries of counter-insurgency operations and imperial policing, where coercive capability is held in the offing and forces on the ground present a more benevolent appearance. The French and British armed forces are not necessarily less violent, but aggressiveness is not their main method of controlling conflict. The French and British approach to peacekeeping differs from what has been incorrectly referred to as the "Scandinavian" method. It is more comprehensible than the US strategy, nevertheless, when applied to countries with

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

gendarmerie-only militaries and philosophies that see coercion as a contributing factor to rather than a remedy for the "cycle" or "spiral" of violence.

Input factors

The following input factors shape doctrine:

i. **The National Interest and National Military Objectives:** What are the government's goals for the military in terms of the national interest and national military objectives? The resources available for defense and the strategic goal in the case of a war will set limits on these aims.

ii. **The Perceived Threat:** A precise and unambiguous assessment of the danger that troops are anticipated to encounter is essential to doctrine. The purpose and/or capacity of a prospective opponent in particular might change, which could have a significant impact on present doctrine and prompt a quick reevaluation and revision of doctrine.

iii. **Politics/Policies:** In a country where the armed forces are subject to democratic authority, the government's intentions take precedence. Changes to a government's security plans, defense strategy, and political institutions will all have an impact on doctrine.

iv. **Experience:** The historical lessons are a key component in the creation of doctrine.

v. **Theory:** Strategists' and theorists' works continue to have an impact on doctrine. Any study of combat may benefit from reading the works of Sun Tzu, Clausewitz, and Jomini, for instance. This does not imply that a single theory can be applied to all possible situations, since history demonstrates that every war will be unique and hence provide unique lessons for the future.

vi. **Education:** Conflict studies help people become better war and conflict commanders. This personal preparation should be continued by everyone engaged in the direction, organization, and conduct of military operations.

Once doctrine is established, it will continue to influence and affect all forces' daily actions. Four distinct categories may be made from the output of doctrine:

i. **Organization:** he defenses organization must accurately represent the military goals of the country and the means by which they will be accomplished.

ii. **Force Structure:** The best way to describe force structure is the combination of personnel, weapons, supporting systems, and equipment that is assigned to carry out certain missions.

iii. **Training Requirements:** Training and exercises must accurately represent the doctrine in effect at the time and integrate any lessons learned in the creation of new doctrine.

iv. **Plans:** Plans are the most detailed result of the doctrine process, and although they should represent current doctrine, they may need to be modified to account for variations in context and situation.

Chinese Doctrine

After examining China as the following country. In order to counter the United States' military technology superiority, China began to create doctrine in 1999. Several of their top strategists released a report titled "Unrestricted Warfare." They were already considering the value of network warfare, which was insightful, but quotes like "Technology is like ‘magic shoes' on the feet of mankind, and after the spring has been wound tightly by commercial interests, people can only dance along with the shoes, whirling rapidly in time to the beat that they set," illustrate how differently a culture can influence how doctrine is developed. Taiwan keeps a close eye on Chinese tactics and recently issued an insightful analysis of a new doctrine the People's Liberation Army (PLA) is considering. The main important ideas are included in the list below [3], [4]:

i. Highly controlled warfare is a novel style of conflict in which "the direct aim is to control a political regime, and in which political, economic, diplomatic, and other resources are effectively

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

integrated to control the scale, form, and results of the conflict, with the support of absolute military superiority."

ii. Acupuncture war, which establishes the inspection of key nodes in a network that, similar to pressure points in martial arts, may shut down a whole system if hit. Electronic warfare (EW) in modern warfare enables "the first battle being the final battle."

iii. Strategic information warfare, which is the fusion of political, economic, military, diplomatic, and other spheres to generate an all-encompassing information triumph. Targets of strategic information warfare (IW) range from single armed systems like aircraft carriers to critical national political, financial, communications, and other sectors.

iv. Company websites, which feature built-in databases and remote learning capabilities for easy access to knowledge that wasn't always accessible.

v. The "Intangible War," which is concerned with tactics, commercial rivalry, legal frameworks, and intellectual property rights. The West cannot afford to ignore these crucial sectors.

vi. Net Force is a novel "Grand War" strategy that integrates high-tech expertise with politics, economics, psychology, and information networks. Its goals include "all people becoming warriors," the integration of peace and conflict, and dual use for the military and civilians."

vii. Surgical warfare, or targeting one point to bring down the whole system, intends to exploit the weakness of high-tech military systems to secure the decisive victory.

viii. The capacity to disrupt or destroy an enemy's space systems adds the finishing touch to China's asymmetric warfare capabilities under item number.

The report is titled "US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." "The People's Republic of China (PRC) government is a decade into a broad military modernization program that has fundamentally changed its capacity to fight high-tech wars," it reads. The Chinese military is moving away from its traditional missions centered on Taiwan and towards a more regional defense posture employing more networked troops capable of communicating across service arms and across all echelons of command. The doctrine of fighting "Local War Under Informant-ionized Conditions," which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in the air, at sea, in space, and across the electromagnetic spectrum, serves as the foundation for this modernization effort, known as Inform-ionization. This open source analysis demonstrates the seriousness with which China is modernizing its cyber forces in preparation for both the current cyberwar and the upcoming combined kinetic/non-kinetic conflict.

According to the 2011 Annual Report to Congress on Military and Security Developments Concerning the People's Republic of China, China's growing cyberwarfare capabilities are in line with reliable PLA military documents. Information warfare (IW) is a critical component of establishing information supremacy and a successful strategy for thwarting a more powerful adversary, according to two military doctrinal works, Science of Strategy and Science of Campaigns. Both documents encourage the development of skills to compete in this space, despite the fact that neither one specifies the precise requirements for using a computer network assault against an enemy [5], [6].

According to US cybersecurity researchers and specialists, as few as 12 distinct Chinese organizations, mostly supported or led by the Chinese government, are responsible for the majority of the country's cyberattacks that steal crucial data from US businesses and government organizations. The aggressive yet covert assaults that steal data and intellectual property worth billions of dollars often have distinctive marks that enable US authorities to connect them to specific hacker teams. Analysts further claim that the US often assigns the attackers special names or numbers and sometimes has access to information about the hackers' identities and whereabouts. Although political posturing and allegations may follow this targeting, no military action has been authorized as of yet. Similar to the Cold War, it focuses more on intelligence collection,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

but unlike the Cold War, when military might be demonstrated as a show of power but was seldom put to use, many cyber weapons are already in operation.

Finally, the name and location of the primary Chinese Cyber War operation have been revealed via Wikileaks papers and a number of other sources. The Chinese Army's electronic warfare organization in Chengdu, central China, known as the First Technical Reconnaissance Bureau (1st TRB), is the most often identified source of hacking attempts. The 1st TRB still makes use of the servers that were put up more than five years ago. The mounting body of information around operations like the First TRB is categorically refused to be discussed by the Chinese government. Therefore, it is clear that China conducts cyber operations employing both civilian hackers and military Computer Network Attack units.

What are the implications of all this attention on modernization and cyber doctrine? The degree of effort and the nature of the aforementioned efforts demonstrate China's readiness to use the electromagnetic spectrum to reach its adversaries and wage the next war. They will target that point of concentration because they understand how reliant the West has grown on its IT infrastructure. They have the edge today since they are doing reconnaissance. They are equipped to launch denial-of-service assaults. So that their adversary cannot rely on their command-and-control systems to provide reliable reports, they have discussed assaulting the integrity of systems. Although not the only country with this degree of cyber warfare doctrine development, China is at the front of the pack.

Other Asian countries

Japan has assigned responsibility for its strategy to the Self-Defense Forces National Information Security Centre (NISC) of the Japanese Ministry of Defense (MoD). NISC was founded in 2005 as a result of an increase in cyberattacks. The federal agency was established to coordinate efforts to safeguard computer networks. Japan's government approved the Second National Strategy on Information Security (NSIS) in February 2009 for the period 2009–2011. The national and local governments, essential infrastructure, commercial entities, and people are the four topics covered by the three-year plan. In accordance with the NSIS procedure, the Japanese government approved "Secure Japan 2009." One-fourth of its 212 policy recommendations are geared at strengthening national and local governance. The government gives assistance while private businesses serve as the targets of its efforts in the sectors allocated to crucial infrastructure and commercial entities. Japan is creating a comprehensive government-focused cyber policy because they want to protect their nation against assaults and are prepared to use their military resources to do so.

North and South Korea: In December 2009, South Korea's Ministry of National Defense (MND) and Defense Security Command (DSC) said that hackers had acquired secret military blueprints created by South Korea and the US. Information from "Operation Plan 5027," which describes how South Korea would be protected in the case of conflict, was allegedly moved to a Chinese IP address, although it was believed to have been hacked. The ministry's response was to establish a cyber-warfare command to safeguard its military's computer networks. These plans are a component of the ministry's "Defense Reform 2020" policy. Also established was the Korea Internet & Security Agency (KISA) [7].

On the North Korean side, Unit: 121, which was established in 1998, has developed capabilities. By developing its asymmetric and cyber warfare capabilities via both offensive and espionage techniques, the goal is to improve their military position. The Pyongyang-based Mirim Academy trains this unit. An estimate of their yearly budget is $56 million. It is understandable why they would take the conflict online given the ongoing hostilities on the Korean Peninsula. North Korea may have an edge in that they are less reliant on IT infrastructure than other nations, but they will still have a long way to go to make up for the absence of a computer workforce to draw upon.

Although terrorists don't have a clear stated ideology, they are particularly interested in learning about that of the nations they seek to target. Knowing how a country will react to a certain assault would be crucial for strategizing which strikes would be most effective. Additionally, they use the internet for recruitment, communication, and reconnaissance thanks to a number of locally established ideological practices. Finally, it should be presumed that they are aware of how heavily the western nations rely on cyberspace and have aggressively sought out the skills necessary to exploit this weakness, albeit no plans have yet been discovered for how they intend to do so.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

DISCUSSION

To improve the North Atlantic Treaty Organization's (NATO) capacity for cyber defense, the Cooperative Cyber Defense Centre of Excellence (CCD COE), based in Tallinn, Estonia, was officially founded on May 14, 2008. On October 28, 2008, the Centre was granted full NATO recognition and was given the title of International Military Organization. The organization's goal is to improve cyber defense capabilities, collaboration, and information sharing among NATO, NATO countries, and Partners via education, research and development, lessons learned, and consultation. NATO's cyber doctrine will be able to be integrated thanks to this center. Working in a global task force involves resolving political, legal, doctrinal, and technological challenges. This feature has taken years to build in the actual world, and NATO is working to establish it in the virtual world [8]–[10].

CONCLUSION

Additionally, the UK is creating cyber doctrine and plans. The UK Office of Cybersecurity and UK Cybersecurity Operations Centre announced the "Cybersecurity Strategy of the United Kingdom safety security and resilience in cyber space" in June 2009. There is continuous and widespread discussion over what "cyber warfare" may entail, according to this text, but there is agreement that with a rising reliance on cyberspace, the defense and exploitation of information systems are crucial challenges for national security. In order to guarantee that we can defend against an assault and intervene against enemies when required, we recognize the necessity to enhance military and civil capacities on a national and international level. States, terrorists, and criminals are also included here, whether they are using it for military, political, or even espionage purposes. The UK has made it quite obvious that it is addressing this as an issue of national security by acknowledging that cyberwar is a real possibility and that they are preparing for it. Although they consider them as distinct from combat, they broadened the definition of the cyber battle field to include criminal activity and espionage. This inclusion in the statement demonstrates the overlap that is one of the problems with cyber doctrine.

REFERENCES

[1] J. Rineheart, "Counterterrorism and Counterinsurgency," Perspect. Terror., 2010, doi: 10.1080/15027570802277813.

[2] F. N. Pieke, "Party spirit: producing a communist civil religion in contemporary China," J. R. Anthropol. Inst., 2018, doi: 10.1111/1467-9655.12913.

[3] B. Ganor, "Four questions on ISIS: A 'trend' analysis of the Islamic State," Perspect. Terror., 2015.

[4] J. Aspremont, "A Postmodernization of Customary International Law for the First World?," 2018. doi: 10.1017/aju.2018.77.

[5] E. Balla, "European Security Strategy in the 21st Century: The Blair Doctrine Revisited," ATHENS J. Soc. Sci., 2017, doi: 10.30958/ajss.4-4-4.

[6] Z. Jovanovski, A. Iliev, and A. Ilieva Nikolovska, "Historical Perspectives and Legal Aspects of Cyber Warfare," Ann. Disaster Risk Sci., 2020, doi: 10.51381/adrs.v3i2.53.

[7] T. Taylor, "High Command: British Military Leadership in the Iraq and Afghanistan Wars," RUSI J., 2015, doi: 10.1080/03071847.2015.1102559.

[8] M. Špirk, "Mind and body of humanistic buddhism in practice: A case study of the temple and community of fo guang shan vienna," Religio, 2020, doi: 10.5817/REL2020-2-1.

[9] T. A. Lima and M. N. da Silva, "Alquimia, Ocultismo, Maçonaria: o ouro e o simbolismo hermético dos cadinhos (Séculos XVIII e XIX)," An. do Mus. Paul. História e Cult. Mater., 2001, doi: 10.1590/s0101-47142001000100002.

[10] R. Johnson, "and Counterinsurgency," J. Mil. Ethics, 2008.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of Some Key Military Principles that Must be Adapted to Cyber Warfare

Mr. Sunil Sahoo, Assistant Professor,
Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-sunilkumarsahoo@presidencyuniversity.in

Abstract: ***The rise of cyber warfare has brought new possibilities and difficulties for military strategists as the field of battle continues to change. This essay examines how important military ideas may be applied to the field of cyberwarfare. This paper analyses and analyses the essential principles necessary for success in cyberwarfare by drawing on well-established ideas like the principles of war, operational art, and leadership. Military organizations may successfully traverse the complicated and quickly evolving field of cyber warfare by grasping these concepts and applying them to the particular features of cyber operations. This will eventually improve their capacity to both protect against and take advantage of cyber threats. Policymakers, military leaders, and cyber experts may learn important lessons from this study as they work to establish comprehensive plans and tools to protect national security in the digital era.***

Keywords: Combatant Controls, Cyber Warfare, Cyber Security, Military Principles, World Wide Web.

INTRODUCTION

The French government released a white paper on defense and national security that states that cyber war is a major concern and that it develops a two-pronged strategy: on the one hand, a new concept of cyber defense, organized thoroughly and coordinated by a new Security of Information Systems Agency under the supervision of the General Secretariat for Defense and National Security; and on the other hand, the establishment of an offensive cyber war capability, part of which is the development of a new Security of Information Systems Agency. This white paper does highlight their conviction that this is a military issue with the necessity for offensive capabilities under their special services groups, even if it is not a national plan. They have adopted the strategy that the majority of nations will use, while only a small number of nations are attempting to incorporate this capacity into their conventional forces. It followed a similar process before being incorporated into tactical actions on the battlefield [1].

The Czech Republic has released their cybersecurity plan for the years 2011 to 2015. "Essential objectives of the cybersecurity policy include protection against threats to which information and communication systems and technologies are exposed, as well as mitigation of potential consequences in the event of an attack against ICTs," the document states. The goal is to maintain a safe, secure, resilient, and credible environment that takes advantage of the opportunities provided by the digital age. The Czech Republic has a duty to implement, operate, and secure credible information and communication systems. This duty extends to all levels of government and administration, the private sector, and the general public. The plan coordinates with other relevant strategies and ideas and focuses primarily on unhindered access to services, data integrity, and confidentiality of the Czech Republic's cyberspace. It's important to note that they want the general public to contribute to the solution.

Private or Mercenary Armies

Gen. Michael Hayden said on August 1, 2011, "It may be necessary for the private sector to stop playing defense and go on offence in an age where cyber warfare is more prevalent than the actual battlefield." During a panel discussion at the Aspen Security Forum in Aspen, Colorado, Hayden, who oversaw the National Security Administration and the Central Intelligence Agency under President George W. Bush, said that there has been precedent for such action and that the federal government may not be the only defender of private sector companies. When that happens, he said, "we may reach a point where defense is more actively and aggressively defined even for the private sector and what is

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

permitted there is something that we would never let the private sector do in physical space." How about a digital Blackwater, I'll really toss up a bumper sticker for you, he said. In terms of what we expect the government to do or will allow the government to do, "I mean, we have privatized certain defense activities, even in physical space, and now you have got a new domain." Private military contractor Blackwater has changed its name to Academy after receiving a bad reputation as a result of events in Iraq. Companies hiring troops (hackers) to execute retaliation or recovery operations might significantly alter the internet battlefield.

To put ideology into practice, a variety of tactics, techniques, and procedures (TTPs) are utilized. The Joint Munitions Effectiveness Manual (JMEM) factors, Measures of Effectiveness (MOEs), Battle Damage Assessment (BDA) to ascertain whether MOEs were achieved, Close Air Support (CAS) to integrate air and land forces, and Counterinsurgency (COIN) to adapt the traditional force on force doctrine to asymmetric battlefields are some of the fundamental TTPs [2].

Intelligence Preparation of the Operational Environment (IPOE)

In today's complex battles, intelligence preparation of the operational environment, or IPOE, has replaced intelligence preparation of the battlefield (IPB). The combined intelligence organizations utilize it as "the analytical process to develop intelligence estimates and other intelligence products to assist the joint force commander's decision-making process. It is a continual process that involves identifying the operating environment, outlining its effects, assessing the enemy, and figuring out the adversary's next steps. This calls for assessing not just the usual geography and adversary capabilities, but also a wide range of new demographic factors, including as economic, racial, religious, gender, ethnic, and cultural ones. It is now vital to integrate cyberspace in the examination of lines of communication, influence operations, and terrain. To remain inside the enemy's OODA loop (Observe, Orient, Decide, Act), cyber IPOE is essential. "To be valuable, IPB must be: timely, accurate, useable, full, and relevant. Typically, 80% of the fundamental groundwork must be finished before operations and logistics can begin planning. Therefore, IPOE must reevaluate how it creates products like "enemies most likely course of action," but these products are still essential to the commander and must not be disregarded in cyberspace, given that the terrain can change by the minute, forces can be dispersed across the globe, and motives can be as varied as the groups involved.

Joint Munitions Effectiveness Manual (JMEM)

A systematic capability study known as the Joint Munitions efficacy Manual (JMEM) is used to assess the efficacy of various weapon systems, such as whether an AT4 bazooka can kill a T64 tank. These estimates may be produced by field testing or by applying probabilistic mathematical models that take into consideration the target's major vulnerabilities, performance information on the assets being considered for use against the target, and methods of delivery. These forecasts are based on past strike performance statistics and evaluations of expected success given the particular intended weapon / target combinations (such as Air-to- Surface, Special Operations Target Vulnerability, or Surface-to-Surface).

When evaluating kinetic impacts, this is very simple, but there are many other things that may affect how effective a cyberweapon is. In order for a commander to know which submunitions are optimal for their purposes, we need to set a baseline standard to gauge effectiveness. The benchmark will depend on an impact of some kind, such as "time not available" or "ability to influence decision." The Joint Non-Kinetic Effects Integration (JNKEI) project, which was finished in September 2010, included some work on this. To help joint planners include the non-kinetic impacts of electronic assault, computer network attack, and offensive space control capabilities into operational planning, it was intended to build joint TTPs. The following goals were achieved [3], [4]:

i. Greater non-kinetic capability integration during operational planning, which gives combined force commanders more options for future action.
ii. Information exchange needs based on the JNKEI TTPs and included into the collaboration tools Virtual Integrated Support for the Information Operations Environment (Vision) and Integrated Strategic Planning and Analysis Network (ISPAN).
iii. Contributions were made to the Joint Publications (JP) 5-0, Joint Operational Planning, JP 3-13, Information

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Operations, and JP 3-60, Joint Targeting.

iv. JNKEI TTPs were given to the Advanced Integrated Warfighter Weapons Instructor Course (US Air Force Weapon School), Joint Targeting School (Joint Forces Staff College), and Joint Information Operations Planning Course (Joint Forces Staff College).

v. USEUCOM, USPACOM, US Force, Korea, and USSTRATCOM received v. JNKEI TTPs to improve current standard operating procedures.

Measures of Effectiveness (MOE)

The assessment of changes in system behavior, capacity, or operational environment that are linked to assessing the fulfilment of an end state, the accomplishment of an aim, or the production of an impact is known as a measure of effectiveness (MOE); task performance is not measured by MOEs. We must consider the effect or MOE of a course of action or combat evaluation while assessing it. To avoid creating the misleading appearance that a job or aim has been completed, these MOEs should employ assessment metrics that are pertinent, quantifiable, responsive, and resourced. If we are discussing influence operations or information operations, this may become quite complicated. We must develop a benchmark by which every military branch and government agency evaluates both impact and effectiveness. It will need to be a matrix that can handle breaches in confidentiality, access restrictions, and integrity issues and represents the effects on the impacted national power (military, economic, informational, or diplomatic). It should be carried out in an unclassified manner so that everyone may practice using it until everyone is familiar with it [5].

Battle Damage Assessment (BDA)

A crucial TTP is Battle Damage Assessment (BDA). It is an assessment of the harm brought about by the use of deadly or non-lethal military action. Physical damage evaluation, functional damage evaluation, and target system evaluation make up battle damage assessment. The goal of BDA is to contrast the outcomes of the execution with those that were anticipated or forecasted during target development. Joint force intelligence and operations elements must work together in a coordinated and integrated manner to implement comprehensive BDA. Physical damage assessment, functional damage assessment, and functional evaluation of the next higher target system make up BDA traditionally. To ascertain if the assault approach has an effective MOE, BDA is essential. Air Force aircraft would not take off until it was certain that the enemy's anti-aircraft guns had been destroyed. Before launching an exploit, cyber troops would need to be sure they could get beyond the protective firewalls. In order to provide proper analysis, it is often desirable to combine all of the various gathering capabilities into "all source" information enabling correlation across all Intel Functions.

Close Air Support (CAS)

Air action by fixed- and rotary-wing aircraft against hostile targets that are in close proximity to friendly troops requires careful integration of each air operation with the firing and movement of those forces. This is known as close air support (CAS). This TTP serves as a reminder that integrated forces are more potent than unintegrated ones. A cyberwar will very certainly be part of an integrated operation involving various facets of state power, as the US does not fight wars alone but rather as a member of international coalitions, the Army seldom engages in combat alone but rather as a member of a Joint Task Force [6].

Counterinsurgency (COIN)

Counterinsurgency (COIN) refers to extensive civilian and military actions used to thwart and control insurgency while resolving its primary grievances. Security is only one of a vast number of operations that make up COIN, which is essentially political in nature. To undertake COIN operations effectively, all Host Nation (HN), US, and international agencies or players must work together. The most frequent kind of war in which the United States has been involved recently is insurgent suppression. Information operations and influence operations are important force multipliers in this kind of setting. Both sides' use of cyber is essential in this form of conflict. Commanders must comprehend how to rule online as they consider how to fight and prevail on today's battlefield. If we push the staff functions to concentrate on the correct criteria, the same weapons they use to combat on the local battlefield may be converted to be utilized in cyberspace.

Situational Awareness to Information as Contested Terrain

Cyberspace is not necessarily a brand-new or

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

nonphysical concept, nor is it a completely new domain of conflict. Actually, it is entirely physical, just like any other terrain. The emergence of cyberspace as a disputed realm has profound effects on military strategy. The strategic knowledge of effects, such as situational awareness, which involves clearing the commanders' present comprehension of the circumstances of the fog of war, are almost unintelligible. The strategic and cognitive effects on a leader's capacity for planning and executing should be significant. The use of computer information technology in both offensive and defensively military operations is known as command-and-control warfare. Command and control warfare is an improvement to the military unit's operational capability rather than its principal way of operations. A commander's authority over cyber resources might likewise be exploited against him or her. As a result, there is a natural connection between the combatant commander and the communication infrastructure. It may be crucial to remember that information technology and computers exist at all levels and are not limited to the desktop personal computer, despite the desire on the part of technologists to use the term computer information technology. Additionally, a lot of military radios and encryption systems include computers. Information technology and computerized capabilities bring with them a new set of hazards that must be weighed against the benefits of the new technology. Some technology critics can exaggerate the dangers. The prevalence of "collapse theory" as the main concern linked with developing information technology is one aspect that is probably overblown. Systems for communications and computation at a large scale are constructed with redundancy and expandable capacity. It is feasible to overwhelm these systems, but the collapse hypothesis postulates that they will not be able to bounce back [7], [8].

DISCUSSION

On the current battlefield's high intensity combat terrains, the act of surprise becomes more challenging. The most recent invasions of other sovereign territory by domestic and international forces have been preceded by protracted buildups, giving the impression that a pressure cooker is finally letting out steam. The fact that it took so long rather than truly being sneaky may be described as surprising. Cyber warfare's use of computer information technology makes it quickly clear that many assaults occur every day. Numerous literary authors that discussed the absence of security previously provide evidence to this. Therefore, surprise and present terrestrial conflict have a lot in common. The binary contains simplicity. The binary of on-off that powers computers is one of the simplest things there is. The systems of systems debate mentioned in the literature, which claimed that highly scalable, enormous systems are made with severe security flaws, refutes that claim. According to the literature, simplicity helps the enemy via the other principle of economy of power, and the attacker benefits while the defense is on the other side of the coin from simplicity. Through cascading systems failure and a systems-of-systems design approach, the concept of simplicity as outlined in the literature must favor the attacker over the defense [9]–[11].

CONCLUSION

When examining cyber warfare, it is clear that there is a significant divergence between the traditions of land combat and the concepts of war that comprise strategy and tactics. In actuality, some people only assert its nonexistence. The agreements governing land combat often make reference to the rules of land conflict, such as in the Geneva Convention, suggesting a gap between the legal, moral, and ethical factors. However, in order to address how the methods and ideas for generalized approaches to situational awareness may be carried out, the author chose to concentrate mostly on the second component of the study topic. We were able to discuss a range of assaults by omitting the first half of what the law of war defines as an attack. The discussion in this article provides a solution to the question of assault by focusing on the several sorts of attack that were feasible. One reason for this is that information security perfidy and jus in bello haven't been well defined. Simply said, the whole first portion of the original study topic is compromised by the usage of the civilian network, which is almost a prerequisite. According to the description, the civilian network component increases the danger of perfidy and laws of war breaches in every strike. Finally, as was previously explained, the final component of the issue of how this instrument differs is readily addressed. The asymmetric advantage that the assault has cannot be significantly altered. The nation state is no longer necessary for the amount of effort to join the field of combat. As a result, when a first responder is incorporated into a corporate or military information business, the scale of their

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

assault capabilities dramatically empowers them, but they lack any genuine defense capability. This is the asymmetric advantage that, under scaled systems, does not seem to be eroding at the moment.

REFERENCES

[1] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," Comput. Secur., 2015, doi: 10.1016/j.cose.2014.11.007.

[2] A. Claver, "Governance of cyber warfare in the Netherlands: an exploratory investigation," Int. J. Intell. Secur. Public Aff., 2018, doi: 10.1080/23800992.2018.1484235.

[3] R. S. Shaji, V. Sachin Dev, and T. Brindha, "A methodological review on attack and defense strategies in cyber warfare," Wirel. Networks, 2019, doi: 10.1007/s11276-018-1724-1.

[4] A. Ibrahim, N. Mahmud, N. Isnin, D. Hazelbella Dillah, and D. Nurfauziah Fauz Dillah, "Cyber Warfare Impact to National Security - Malaysia Experiences," KnE Soc. Sci., 2019, doi: 10.18502/kss.v3i22.5052.

[5] S. Goel, "How improved attribution in cyber warfare can help de-escalate cyber arms race," Connections, 2020, doi: 10.11610/Connections.19.1.08.

[6] K. E. A. Tampubolon, "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare," Jurist-Diction, 2019, doi: 10.20473/jd.v2i2.14250.

[7] A. Zotti, "Inside cyber warfare," Glob. Chang. Peace Secur., 2011, doi: 10.1080/14781158.2011.605638.

[8] A. Ween, P. Dortmans, N. Thakur, and C. Rowe, "Framing cyber warfare: an analyst's perspective," J. Def. Model. Simul., 2019, doi: 10.1177/1548512917725620.

[9] H. P. Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century," Baltic Journal of Law and Politics. 2017. doi: 10.1515/bjlp-2017-0001.

[10] B. Pratama and M. Bamatraf, "Tallinn manual: Cyber warfare in Indonesian regulation," in IOP Conference Series: Earth and Environmental Science, 2021. doi: 10.1088/1755-1315/729/1/012033.

[11] V. Duddu, "A survey of adversarial machine learning in cyber warfare," Def. Sci. J., 2018, doi: 10.14429/dsj.68.12371.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of Tools and Techniques for Cyber Warfare

Mr. Ramakrishna Konnalli
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-ramakrishna@presidencyuniversity.in

Abstract: ***The array of technologies available for use in penetration testing, cyberwarfare, and security in general is absolutely astounding. Although it would have been fantastic to be able to provide a thorough analysis of the many widely used security technologies, we would have needed to dedicate an entire book to it. Additionally, it is important to note that although hackers may spend a few thousand dollars, certain nations such as the USA with the National Security Agency and Comprehensive National Cybersecurity Initiative spend billions. We cover some of the highlights in this chapter, but for those who are interested in learning more, Insecure.org is an excellent resource. They keep listings of wireless tools, vulnerability scanners, web scanners, sniffers, password crackers, and many more useful tools.***

Keywords: Cyber Warfare, Cyber Security, National Security, Organization, World Wide Web.

INTRODUCTION

Despite being acknowledged as the new battlefield in the information age, cyberspace still lacks a universally agreed-upon description. Cyber weapons operate in a similar manner. In his book, Cyber War, US Government security expert Richard A. Clarke describes cyber warfare as activities taken by a nation state to infiltrate the systems or networks of another country with the intention of inflicting harm or disruption. As a result, cyber weapons are the equipment used in cyberwarfare. In their most basic form, weapons may be described as "instruments of harm". Humans have used weapons to hunt, defend themselves, and obtain power from the beginning of time. With the development of technology and the necessity to eliminate the perceived danger, the variety of weapons and their range, lethality, and accuracy have significantly risen. As a result, weaponry have changed throughout time. With the speed at which technology is developing and being put into production, it has become easier to turn a notion into a physical object or weapon. Although at a far higher rate than traditional weaponry, cyber weapons are also developing. In the realm of cyberspace, advancements in technology may place in days or even hours, and new dangers quickly follow. The Stuxnet strike on the Iranian nuclear facilities served as a major example of how far-reaching the use of cyber weapons has become [1].

Logical Weapons

When we talk about software or tools in cyber warfare, we probably picture logical weapons. These are the tools used for reconnaissance, which includes looking into the networks and systems of our adversaries before attacking or exploiting (which, in terms of CNE, means spying on) any potential targets we may come across. We could wonder how these techniques vary from those used in routine penetration testing of apps, systems, and networks when we consider their employment in the context of cyberwarfare. The answer to this is that, although they are often theoretically similar in many circumstances, the purpose and effect of their employment are frequently much enhanced in a cyber-warfare scenario [2].

While some contracts may require penetration testers to avoid "dangerous" tools or settings because of the potential negative consequences on the target at the other end, such impacts may be acceptable or even desired in a cyber-conflict. This may not always be the case, and in certain circumstances, we may still want to be discreet and careful, but it does allow for the use of standard tools in ways that penetration testing outside of a lab setting does not often allow for. Commercial tools may very well be in the hands of cyber warfare forces supported by or employed by nation governments, but it is less probable that they

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

will be in the hands of lone people or small groups. Although less automated than some of the commercial tools, the free tools may nevertheless be quite powerful in the hands of an experienced attacker and are often used by different types of attackers.

Reconnaissance Tools

As should be obvious from the name, reconnaissance tools are those that we employ to acquire data, often in a passive state, about the networks and systems that we may intend to take rational action against. These efforts might include gathering data from open-access websites, researching Domain Name System (DNS) server records, gathering metadata from papers that are available, using search engines to find very precise information, or any number of other related tasks. For scouting, we may make use of data acquired from sources like:

a) Websites.
b) Search engines.
c) Google hacking.
d) WHOIS searches/DNS queries.
e) Metadata.
f) Specialized search tools such as Maltego.

Scanning Tools

The group of tools we employ to learn more about our target environment, the systems inside of it, and the specifics of those systems is known as scanning tools. With these tools, we may be fairly generic when doing ping sweeps, a little more precise when performing port scans, or highly specific when capturing banners or counting users on specific systems. Some typical scanning devices include [3]:

a) Nmap.
b) Nessus.
c) OpenVAS.

Access and Escalation Tools

Many of the hacking and penetration testing tools that are now available, both commercial and free source, are geared on getting access to systems and increasing the amount of privilege after we have done so. In this part, we'll discuss a few of the most prevalent and well-liked tools. Tools for common access and escalation include:

a) Password cracking/guessing tools.
b) Metasploit.
c) CANVAS.

Exfiltration Tools

Exfiltration of data from an environment may be a fascinating and difficult topic, especially if the environment is guarded against the same actions that we are trying to do. In broad strokes, some of the primary techniques we may use to exfiltrate data include physically transporting the data, disguising the data using steganography or encryption, using widely used protocols that are often permitted to leave the environment, or using out-of-band techniques. Typical techniques for exfiltration include:

a) Physical exfiltration.
b) Encryption and/or steganography.
c) Tunneling over common protocols.
d) Out-of-band (OOB) methods.

Sustainment Tools

We will probably want to make sure that we can access a system in the future after we have gotten access and attained the necessary degree of access. Although we may have been enabled to successfully access the system using a certain weakness or related techniques in the past, we cannot rely on the same flaw to be present in the future. Some typical strategies for maintaining access include [4]:

a) Adding “authorized” accounts to systems.
b) Backdoors.
c) Adding listening services.

Assault Tools

There are a wide range of tools that may be used to attack a hacked system. Simple configuration or environment variable modifications to a system, as well as purpose-built botnets that may launch a concentrated Denial of Service (DoS) assault against a specific system or environment, are just a few examples of how they might manifest themselves. Such destructive tools may often be divided into those focused on hardware or those connected to software. Typical attack techniques could include:

a) Tampering with software or operating system settings.
b) Attacking hardware.
c) Changing configurations.

Obfuscation Tools

Obfuscate is a verb that meaning to obscure, bewilder, or stupefy as well as to make obscure or ambiguous. The collection of tools we may use to hide our traces while working on a system or in an environment are fully suited by this concept. Obfuscating our location, altering logs, and manipulating files are the three major job categories that we are often concerned with

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

in such situations. Some techniques for obfuscation may be: Obscuring physical location.

a) Log manipulation.
b) File manipulation.

Physical Weapons

Most likely, when we think about cyber warfare, we picture hordes of super-nerds glued to banks of monitors, frantically tapping away on their keyboards. Although this specific mental image may have some element of reality, we also need to take into account the role that conventional combat plays in these battles.

The intersection of the physical and logical worlds reveals how intertwined they really are. Software and other logical systems are fully reliant on the infrastructure and physical systems on which they function. Changes to the logical or physical components may have a significant impact on one another, sometimes to the point where one renders the other utterly worthless.

We are concerned with the infrastructure, supply chain, and logistics that enable our activities, just like in any significant physical battle. At best, fighting becomes much more difficult if one of these elements is destroyed or undermined by hostile troops. At worst, supply chain problems like tainted egg salad served in a mess hall or cafeteria or subversion of the components required to assemble electrical or computational equipment may render us completely unable to take action [5], [6].

We have a broad range of alternatives when it comes to the instruments we may utilize for physical assault and defense. We can pick locks, break wires, jam communications, use conventional explosives, and pretty much anything else that comes to mind. We can take precautions to ensure that any attackers who do manage to breach our perimeter are swiftly recognized and thwarted in their endeavors, and we can harden our facilities and equipment against the assaults we believe to be most probable.

Connection of the Logical and Physical Realms

Most people with a rudimentary level of technological understanding are aware that the logical world relies on physical hardware and network infrastructure. Despite the fact that the concept of the virtual world riding on the real world is straightforward, some of the second-order impacts of crossovers between these two worlds may not be as evident or clear-cut.

In cyber operations, keeping our own systems and infrastructure intact and capable of performing as intended, and making the adversary's systems and infrastructure incapable of doing so, are our two main concerns when looking at the physical network infrastructure on which such systems are maintained. Therefore, a physical assault on the data center is a possibility for military denial of service strikes.

The physical world may be changed using logical systems as well. Software often controls how sophisticated pieces of physical hardware operate. Modifications to the software may have an impact on any networks, other systems, or even humans that the hardware interacts with. This implies that a cyberattack on the electrical infrastructure may also be used to degrade service to the data center.

Logical Systems Run on Physical Hardware

The logical world is supported by a range of embedded technologies, including network infrastructure, computers, home automation technology, refrigerators, vehicles, and more. When a complicated gadget loses access to the numerous services essential to its operation, namely power and communications channels, it loses a lot of functionality and is often reduced to the status of a very costly paperweight. Keeping the actual gear that supports such activities operating may be difficult while performing operations in a cyber-conflict, whether offensive or defensive. Even in conventional combat, a component of cutting-edge technology has started to make an appearance, and the data it provides may provide crucial information on which to base both conventional and cyber operations.

Recent American military operations, such as those in Iraq and Afghanistan, sometimes took place in scorching, sand-covered desert regions without much in the way of infrastructure already in place. Operating in such settings is often not ideal for maintaining the operation of computer hardware. As they are essential to US command and control, such equipment may also provide a tantalising target for hostile forces to assault, both physically and logically. In these circumstances, it is often necessary to use portable cooling systems and ruggedized equipment in order to have any confidence in the devices' long-term functionality. At a higher level, we also need to maintain the infrastructure that these systems depend on. Although it is not often hardened to resist the kind of assault we could encounter in a cyber-conflict, such technology is frequently found in data centres and other locations that house crucial computer equipment. We may make

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

it exceedingly challenging to shut down systems by employing redundant systems, infrastructure, utilities, and other similar demands. However, given that these technologies are widely accessible, it is possible that our competitors will use them as well [7].

The issue of trying to physically disable the infrastructure and equipment of the opposing troops lies on the other side of this one. Those who are being attacked could have a clear "home court" advantage, especially when actual actions are taking place on foreign land. In certain circumstances, such as the Afghan battle, we can be up against a foe that completely lacks a sophisticated technology infrastructure. In other situations, we could be dealing with robust data centers that have been fortified and have enough backup resources to provide power and communications in an emergency. These can be quite difficult to take down. Each adversary theatre of action will differ in its dependence on and capacity for supporting net-centric operations, necessitating individual evaluation.

It took many rounds of cruise missiles during Operation Iraqi Freedom in 2003 to disable the Internet in Baghdad. Although it was very simple to shut down the civilian Internet Service Providers (ISPs), with most of the traffic coming from a single Cisco switch, the traffic from the Iraqi government was more difficult to quiet. The main Iraqi government website and the related email server were shut down after direct strikes on two telecom switching centers, multiple satellite dishes and a server located in the Iraqi Ministry of Information building. Later, it was out that communications were being sent via a satellite gateway that the manufacturer had first sent to Dubai and then transported into Iraq. This demonstrates how challenging it is to map threats to important infrastructure nodes and the cyber environment.

Given how simple it is to build backup systems on various infrastructures, it is quite likely that numerous systems would need to be brought down in order to disable an opponent's cyber capabilities. Internet access may be delivered by phone lines, microwave, mobile, ham radio, and a number of other technologies. It can also be shared via mesh networking, which allows for a high level of redundancy. With the capabilities of today, a system may even be constructed to run on a laptop and a data connection via a mobile phone. To totally take down a system under such circumstances, a mix of physical and logical assaults may be necessary [8].

DISCUSSION

In the same way that logical assaults may impact physical systems, physical attacks can impact logical systems. The operating systems and applications that are installed on physical computer devices largely determine how they function. For a very simple illustration, practically all systems that are physically linked to a network cable may be removed from the network by making modifications to the network configuration. If such a device is taken from the network, communications with it may be resumed using a backup communications technique, or someone would need to go to the device physically to change its configuration. While utilising such an attack to disrupt network infrastructure throughout an organisation might quickly put an entire company to a standstill and be highly time consuming to cure, it may be quite simple and ultimately very simple to solve. Secondary communications networks are also often less secure and may expose the command to spying.

Attacks on physical systems may result in considerably more severe consequences than just inconvenience for network and system operators. The unencrypted wireless signal used to regulate a pacemaker and defibrillator combo was made accessible to security researchers in 2008 with the help of the Universities of Washington and Massachusetts. They were able to change the settings such that it would administer possibly lethal shocks and switch off completely by exploiting this access. Although the assaults used in this area of study were clearly not simple and required a significant amount of research and specialised gear, the idea has now been verified. In 2009, the first pacemaker that was wireless and linked to the Internet was implanted in a patient, making things significantly worse for assaults of this kind in the future. To get back to our earlier scenario, the ability for a certain doctor, say a cardiologist at the White House, to remotely connect to and disable all such devices may have a significant impact on politics [9], [10].

CONCLUSION

These assaults may be used to target vital systems that regulate the elements powering industrial operations all around the globe, in addition to such worries about generic computer devices. These systems manage manufacturing, communications, water and electricity distribution, as well as a variety of other crucial

operations. People who work in the computer and technology industries sometimes think that when we use the term "infrastructure," we are exclusively referring about network infrastructure. While many operations would not work at all without this infrastructure, it is just a small part of the overall infrastructure that supports the industrial world. The systems that really handle these things are the main thing to think about when talking about infrastructure and the related systems. Power, water, communications, industrial procedures, and a variety of other operations are all regulated by these control systems.

REFERENCES

[1] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. Mcfarland, B. King, S. Webster, and B. Tello, "Analyzing Mission Impacts of Cyber Actions (AMICA)," NATO IST-128 Work. Cyber Attack Detect. Forensics Attrib. Assess. Mission Impact, 2015.

[2] H. Blakey, "Designing Player Intent through 'Playful' Interaction," M/C J., 2021, doi: 10.5204/mcj.2802.

[3] M. Stytz and S. Banks, "Cyber warfare simulation to prepare to control cyber space," Natl. Cybersecurity Inst. J., 2014.

[4] B. E. Mullins, "Developing cyber warriors from computer engineers et al," Comput. Educ. J., 2012, doi: 10.18260/1-2--21185.

[5] J. Andress and S. Winterfeld, Cyber Warfare. 2011. doi: 10.1016/C2010-0-66971-9.

[6] A. M. Ronchi, "Fostering the Culture of Cyber Security," 2019. doi: 10.23919/ISTAFRICA.2019.8764870.

[7] N. Kaur and J. Singh, "Network-based attacks and its correlation with Indian cyber laws," Int. J. Control Theory Appl., 2016.

[8] M. B. Hotchkiss, "Russian Active Measures and September 11, 2001," Int. J. Cyber Warf. Terror., 2017, doi: 10.4018/ijcwt.2017010103.

[9] K. Ji-Young, L. Jong In, and K. Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," 2019. doi: 10.23919/CYCON.2019.8756954.

[10] W. C. L. Junior and A. O. De Sá, "Triggering Cyber-electronic Attacks in Naval Radar Systems," 2020.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Introduction of SCADA to Cyber Security

Ms. Shaleen Bhatnagar
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-shaleenbhatnagar@presidencyuniversity.in

Abstract: ***Critical infrastructures are becoming more interconnected, and the use of Supervisory Control and Data Acquisition (SCADA) systems has led to serious worries about cyber security. To reduce the dangers brought on by cyber threats, this study examines the growth of SCADA systems and their vulnerabilities, putting particular emphasis on the need for strong cyber security measures. This paper demonstrates the possible implications of successful attacks and emphasizes the significance of installing strong security measures by looking at well-known cyber security events that targeted SCADA systems. The study also examines several techniques and tools, including intrusion detection and prevention systems, encryption, access restrictions, and incident response techniques, that may be used to increase the resilience of SCADA systems. Organizations may create comprehensive plans to protect critical infrastructure from cyberattacks, maintaining the dependability and integrity of key services, by recognizing the special needs and problems of safeguarding SCADA systems. As they work to improve the cyber security posture of critical infrastructures, policymakers, security experts, and SCADA operators may all benefit from the knowledge provided by this research.***

Keywords: Control Systems, Data Acquisition, Industrial Control Systems, Information Security, Network Security, SCADA Security

INTRODUCTION

Numerous processes are controlled and tracked by Supervisory Control and Data Acquisition (SCADA) systems. These procedures may be infrastructure-based, industrial-based, or facility-based. Industrial processes may entail factories, power plants, oil refineries, mines, or any other number of comparable operations that take place in settings resembling factories. Water and wastewater systems, pipelines used to transport oil and natural gas, the transmission of electrical power, communications systems like landline or cellular phone systems, and other systems that provide goods and services that are typically regarded as utilities all play a role in infrastructure processes. Facility processes are those that control operations in specific facilities, such as energy use or heating and cooling. The military is beginning to create measures to defend against assaults on SCADA systems, which are used by important bases and forts. The Smart program is one example. These systems are appropriately known as Industrial Control Systems (ICS). SCADA systems, Distributed Control Systems, Human-Machine Interfaces (HMIs), Master Terminal Units (MTUs), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and other similar components make up ICS [1]. Instead of using the less common name ICS, these areas are sometimes combined under the heading of SCADA. The main difference between SCADA and ICS centers on the details of what and where is being controlled or coordinated. Such differences across sectors are often not standard, and ICS may technically be more accurate than SCADA in certain circumstances.

Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS).

The majority of the things we interact with have SCADA systems built in. We are just a few steps away from such systems, if not immediately engaging with them, when we fill up our vehicles with petrol, browse the internet, prepare supper, or flush the toilet. Remote sensors are becoming more prevalent in many residential areas because they allow utility providers to read meters more accurately and because they eliminate the need for someone to physically go to each reader to manually gather data. Additionally, they are found in medical equipment that wirelessly updates medical personnel, such as pacemakers, hip replacements, and insulin pumps. Finally, almost all of the weapons that the US military employs today have CPUs. These all provide fresh danger vectors.

We would soon be without heat, food, communications, and many other requirements if such systems weren't in place to maintain and watch over the contemporary world. Without a doubt, these systems are susceptible since they are dependent on

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

computer technology even if they are made for industrial use and, in certain essential systems, are multiple redundant.

Security Issues are Present in the World of SCADA

The majority of SCADA systems rely on security via obscurity. Outside of the industries in which they are used, these systems make use of interfaces, programs, operating systems, and protocols that are not well understood. Theoretically, an attacker would require insider knowledge of the design of the specific, possibly unique system to breach a SCADA system, or they would need to invest the time necessary to obtain access to the system and get familiar with its workings before launching their assault.

Unfortunately, the information era is well underway, and anyone willing to go into the Internet wasteland will find a wealth of knowledge there. Internal documents are leaked to the public, manufacturers simply provide user manuals online for consumers to download, and strange industrial equipment may be purchased on eBay for pennies. We are well beyond the point where we can rely on the opaque nature of a system to transmit any significant amount of security against attackers, even though such systems do tend to be far more customized than the usual server. Indeed, systems and software that have not been put through the ringer of exposure to the Internet and outside attackers may very well be weaker as a result of the manufacturer not being informed of their security problems [2], [3].

As an example, the multi-part malware known as StuXnet, whose primary target is SCADA systems, was found in July 2010. StuXnet is made up of a Trojan that particularly hunts for a certain model of Siemens SCADA systems and a worm that spreads through USB sticks using a Windows vulnerability. A rootkit is also added to thwart detection. The database that the SCADA system utilises as a back end is accessed using a hard-coded password if StuXnet discovers that it is on the Siemens systems. Then, while trying different acts of sabotage, it searches for layout and control files for industrial automation and uploads them to a remote system. StuXnet then waits for further instructions from the distant system [4].

With a suspected origin in Israel, StuXnet has been discovered in SCADA systems in a variety of nations, including China, India, Iran, and Indonesia. The software first seemed to be designed for industrial espionage. The loss of an Indian communications satellite may have been caused by StuXnet, which was subsequently shown to have sought to purposefully destroy such systems in specific situations. In addition to these risks, since SCADA systems are increasingly linked to both public and private networks, we are also subject to the typical forms of assaults that affect many widely used systems. SCADA systems are increasingly vulnerable to distributed denial of service (DDoS) assaults, malware-related side effects, updates that create security holes, and a number of other threats.

The Consequences of SCADA Failures

The potential effects of catastrophic SCADA failures may be fairly wide-ranging. A huge catastrophe brought on by a SCADA failure seems quite plausible given that we are talking about the control systems for electrical power, communications, the flow of petroleum, and other such crucial activities. During the widespread power outage that occurred in 2003, we saw an illustration of the possibility of such a breakdown.

In August 2003, we saw the effects of a SCADA failure that first seemed to be quite small in nature and involved electricity distribution in several portions of the US and Canada. In the end, a software monitoring system malfunction at an Ohio utility firm resulted in a power plant outage in the area. Due to the power plant's collapse, nearby power plants had to be utilized to provide electricity. In such outages, heavily laden electricity wires have a tendency to literally droop, as numerous did. Multiple sagging lines failed because they came into touch with inadequately cut trees at different sites. Operators at Ohio utility firms failed to alert controllers at utility systems in the neighboring states when these breakdowns were happening.

At that moment, Ohio's utility systems start to draw electricity from Michigan's systems, leading to a number of problems as the system tried to balance its load. Additional lines broke in Ohio and Michigan, which led to the shutdown of power plants since there was no demand on them. As the system continued to try to balance itself, more electricity was channeled from east coast facilities, overloading them and forcing them to shut down. Grids in Michigan and Ohio started to become disconnected from one another because of the severe problems with the electrical system. Connections to Canada started to break down as well, and grid instability led to Canada's grids starting to go down. In the end, the impacted grids were in Ontario, New York, New England, Windsor,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

New Jersey, and Philadelphia [5].
55 million people were without electricity and 256 power plants were offline by the conclusion of the outage. If we go all the way back to the start of the issue, the failure of a single monitoring system was what caused this significant problem. Depending on the sector of the economy where the collapse occurs, such circumstances have the potential to cause a great deal of death and devastation. Many militaries are assessing repercussions as a result of the 2003 blackout, which was wholly unintentional but eventually caused by a software error. Such assaults have the potential to cause significant disruption and devastation if they attract the attention of a determined adversary.

Supply Chain Concerns

In addition to the issues with the infrastructure that we have already covered, understanding our supply chain is essential. Many years have passed since the beginning of the globalisation process, which has affected almost all major industries. Many nations import gasoline, raw materials, food, clothes, hardware and components for building infrastructure, as well as a vast range of goods, both big and little, that are much too numerous to list.
While there are many advantages to this, there are also many serious drawbacks, especially when considering the potential for conventional or cyberwarfare. The majority of the components, ranging from individual pieces of equipment to the components from which they are constructed, come from a select number of major manufacturing areas around the world when we examine the infrastructure that we might use to carry out such attacks or, in the opposite scenario, the infrastructure that might be attacked [6].

Compromised Hardware

The threat of gear that has been hacked for tactical or intelligence goals is the main worry. Critical components, including routers, switches, firewall appliances, industrial control units, or any other component, may be specifically designed to fail in response to a specific signal or set of circumstances, include a backdoor, or perform other similar functions. This may severely limit the party that is the target of such assaults or perhaps put them at a severe disadvantage.
The Russian Committee for State Security (KGB) had intentions to steal the blueprints for a SCADA control system and the software that went along with it from a Canadian corporation, according to information obtained by the US Central Intelligence Agency (CIA) in the late 1970s and early 1980s. The device, which was eventually used in a trans-Siberian gas pipeline, allegedly allowed the CIA to introduce malware. A significant explosion is said to have occurred in 1982 as a direct consequence of the installation of the control system that was defective. Although there is considerable disagreement over the veracity of this account, it does serve to demonstrate the issue.
We may examine the instance of Operation Cisco Raider, a two-year investigation conducted by the US Federal Bureau of Investigation (FBI), to demonstrate how simple it is to release such modified devices into the market. In this operation, the FBI dismantled a counterfeiting network that had supplied equipment to the US Federal Aviation Administration (FAA), the US Navy, US Marine Corps, US Air Force, and the FBI itself, among others. Even though this example did not have a military purpose, it provides another illustration of what may be done and is having an economic effect that weakens the US's total influence. In this instance, a substantial quantity of equipment was at stake, and the counterfeiting ring's motive was profit rather than sabotage or espionage. Even with the government programs in place to accomplish just this, it is quite improbable that a few pieces of equipment with changed chips would be discovered under more stealth-focused conditions.

Deliberately Corrupted Components

The introduction of purposefully subpar or corrupted components may result in a much easier supply chain problem than the precisely targeted and timed assaults we outlined above. This is a pretty simple form of attack to execute, especially when looking at equipment containing electrical components. Such failures would be easy to introduce and have a huge impact given the enormous range of components contained in a typical piece of electronic equipment and the many suppliers from whom they are sourced.
The "capacitor plague" that began in the late 1990s is one example of a large number of problems caused by a single defective component. The problem is mostly related to competitive industry espionage amongst capacitor producers. According to reports, multiple Taiwanese capacitor manufacturers purchased the formula for the electrolyte used in capacitor production from a Japanese business. The recipe was flawed and lacking numerous essential ingredients that would typically prevent the capacitor from exploding,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

which was unknown to any of the burglars. While this gave the capacitors a brief window of opportunity to work, it also led to their failure sooner than was often anticipated. Some claim that this issue is still present in the market with products manufactured close to ten years after the first incident.

In this instance, the problem was started by the legal capacitor manufacturer as a preventative measure against the theft of their intellectual property, and it only became out of control because the knowledge was so extensively disseminated. It would be conceivable to create components that were intended to fail in a very precise manner or at a specified time if this were an intentional effort to disrupt the supply chain for electronics components, as we discussed in the preceding section "Compromised Hardware." Such parts may wind up in missiles, tracking devices, aero plane avionics, or any number of other crucial systems.

Non-Technical Issues

There are methods that might be utilized as assaults while talking about supply chain problems that have nothing to do with technological products. A sufficiently determined adversary might encounter a variety of problems with the equipment required to conduct cyberwarfare, and those problems could be very effective in preventing such operations from being carried out. Such disruptions may also be trivially simple to organize and carry out given the capability for executing such operations from centralized places.

An army marches on its stomach, as Napoleon Bonaparte once said. Whether toothpaste, cold medication, drinking water, food, or other consumable commodities are required for our troops to execute operations, they are all subject to contamination, whether intentional or unintentional. There are several instances of how similar events have played out in various nations throughout the world.

One specific brand of spinach was discovered to have *E. coli* O157:H7 contamination in August 2006. 199 persons in 26 states were sick from eating the infected spinach during the end of August, the beginning of September, and the beginning of October, with 51% of the cases necessitating hospitalization. Even though this specific incident was unintentional, its effects were incredibly extensive. A large group of people may get sick or perhaps die if such intentional contamination were to occur, especially in a crowded area like a cafeteria.

Nearly every item that is needed to assist our soldiers, both conventional and cyber, might have similar problems, especially in areas that are not thought to be on the front lines of a specific fight. Security is likely to be considerably laxer in a protected distant area than it is on any battlefield. When done properly and discretely, intentional supply problems are more likely to be ascribed to coincidence than to an explicit assault [7].

Tools for Physical Attack and Defense

We shift to direct fire weapons like machineguns and tanks as well as indirect weapons like artillery and planes as we examine some of the traditional offensive instruments or weapon systems. Defense conjures images of underground warriors and defensive minefields. When we think of reconnaissance, we also think about scouting, espionage, and satellite imagery. The cyberspace battlefield is governed by the same principles as the physical battlefield.

Electromagnetic Attacks

In a setting where cyber wars are occurring and are a component of integrated operations that involve cyber, electromagnetic assaults may be highly helpful. We may take advantage of the fact that such processes often rely on rather sensitive electronics. These devices are vulnerable to electromagnetic pulse (EMP) weapons, transmission jamming, and eavesdropping on their emanations.

DISCUSSION

EMP weapons are a recurring theme in various literature and films, such Oceans 11 and the MatriX, although they are less prevalent in reality. In order to destroy non-hardened electronics, EMP weapons produce an extremely high electromagnetic field. Weapons that use high-altitude electromagnetic pulses (HEMP) or high-power microwaves (HPM) actually exist in military inventories. HEMP devices, which are often created by exploding a nuclear weapon high in the sky, generate an EMP across a large geographic region. Naturally, things have gone out of hand in the sphere of warfare if nations are already firing nuclear weapons into the sky, and we will likely soon have other problems than cyberattacks [8]. The integration of SCADA (Supervisory Control and Data Acquisition) systems with cybersecurity has become an increasingly critical topic in recent years. SCADA systems, widely used in industries such as energy, manufacturing, and transportation, play a pivotal role

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

in monitoring and controlling industrial processes. However, their connectivity to the internet and the use of standard protocols makes them vulnerable to cyber threats. As cyber-attacks on critical infrastructure continue to rise, it has become imperative to enhance the security measures surrounding SCADA systems. One of the primary concerns in the convergence of SCADA and cybersecurity is the potential for unauthorized access and manipulation of industrial control systems. Malicious actors with the intention to disrupt operations or gain unauthorized control can exploit vulnerabilities in SCADA networks. These attacks could have severe consequences, including physical damage, financial loss, and endangering human safety. To address these risks, organizations are focusing on implementing robust cybersecurity measures specifically designed for SCADA systems. This includes the deployment of firewalls, intrusion detection systems, and secure communication protocols to protect SCADA networks from external threats. Additionally, ongoing monitoring and vulnerability assessments are necessary to identify and patch any weaknesses in the system. Moreover, increased collaboration between SCADA experts and cybersecurity professionals is crucial for developing effective strategies to protect critical infrastructure. The integration of security protocols into the design and development of SCADA systems, as well as regular security audits, can help ensure that cybersecurity is prioritized from the outset [9], [10].

CONCLUSION

In conclusion, the convergence of SCADA systems with cybersecurity is a critical undertaking in today's technology-driven world. As SCADA systems play a vital role in monitoring and controlling industrial processes, their vulnerability to cyber threats poses significant risks to critical infrastructure. However, by implementing robust security measures, organizations can mitigate these risks and protect against unauthorized access and manipulation. The integration of security protocols, collaboration between SCADA and cybersecurity experts, and proactive monitoring are key components of a comprehensive cybersecurity strategy. Safeguarding SCADA systems is essential for ensuring the safety, reliability, and resilience of critical infrastructure in the face of evolving cyber threats. By prioritizing cyber security in SCADA systems, we can pave the way for a secure and interconnected future.

REFERENCES

[1] Richard Crowder, “Cyber-Physical Systems - an overview (pdf) | ScienceDirect Topics,” Electric Drives and Electromechanical Systems (Second Edition), 2020.

[2] W. O. Redwood, “Cyber Physical System Vulnerability Research,” Diss. FSU, 2016.

[3] D. Watts, “Security & Vulnerability in Electric Power Systems,” in 35th North American power symposium, 2003.

[4] S. Krit, “Review On The IT Security,” 2016 Int. Conf. Eng. Mis, 2016.

[5] D. Rajeswaran, F. Di Troia, T. H. Austin, and M. Stamp, “Function Call Graphs Versus Machine Learning for Malware Detection,” 2018. doi: 10.1007/978-3-319-92624-7_11.

[6] H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, “Cyber security of smart grid and SCADA systems, threats and risks,” in IET Conference Publications, 2016. doi: 10.1049/cp.2016.0692.

[7] M. Richter, K. Schwarz, and R. Creutzburg, “Conception and implementation of professional laboratory exercises in the field of ICS/SCADA Security - Part I: Fundamentals,” in IS and T International Symposium on Electronic Imaging Science and Technology, 2021. doi: 10.2352/ISSN.2470-1173.2021.3.MOBMU-073.

[8] A. Antonini, A. Barenghi, G. Pelosi, and S. Zonouz, “Security challenges in building automation and SCADA,” in Proceedings - International Carnahan Conference on Security Technology, 2014. doi: 10.1109/CCST.2014.6986996.

[9] C. C. Davidson, “Applying Moving Target Defensive Techniques towards the Security of Programmable Logic Controllers,” 2018.

[10] S. D. Krit and E. Haimoud, “Review on the IT security: Attack and defense,” in Proceedings - 2016 International Conference on Engineering and MIS, ICEMIS 2016, 2016. doi: 10.1109/ICEMIS.2016.7745386.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Physical Denial of Service Attack SCADA

Ms. K Vinitha Dominic
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-vinithadominic@presidencyuniversity.in

Abstract: ***The Physical Denial of Service attack (PDoS) on SCADA (Supervisory Control and Data Acquisition) systems is a concerning threat that highlights the vulnerabilities of critical infrastructure. PDoS attacks aim to render SCADA systems inoperable by causing permanent physical damage to the underlying hardware or by tampering with the system's firmware. Unlike traditional cyber-attacks that focus on exploiting software vulnerabilities, PDoS attacks target the physical components of SCADA systems, disrupting essential processes and potentially leading to significant operational and financial losses. This abstract explores the concept of PDoS attacks on SCADA systems, discusses the potential impact on critical infrastructure, and highlights the urgent need for enhanced security measures to protect against this emerging threat. By understanding the nature of PDoS attacks and their consequences, organizations can better prepare themselves to mitigate and prevent such attacks, ensuring the continued reliability and resilience of SCADA systems.***

Keywords: ***Cyber War, Denial of Service, Data Integration, Internet Security, World Web Wide.***

INTRODUCTION

Users are prevented from accessing a service by a DoS attack that overwhelms either the service's physical resources or its network connections. In essence, the assault overwhelms the service with so much data or traffic that nobody else can use it until the malicious flow is stopped. Sending too many queries to a service in a short period of time might cause it to run out of memory, processing power, or storage space. This is one approach to overtax a service's physical resources. Extreme circumstances might potentially result in physical harm to the components of these resources. Similar to this, a DoS attack might send an excessive amount of connection requests to a service that is being used to interrupt its network connections. Legitimate users' connection requests cannot be fulfilled while these issues are being fixed. A denial of service may also result from a DoS attack that improperly uses a program's resources or a website's network connections by taking advantage of a vulnerability in it [1].

DoS assaults may also be launched by certain viruses. These threats may launch attacks using the resources of infected computers when they infect a computer or other device. A distributed denial-of-service (DDoS) assault occurs when many infected workstations attack the same target. A DoS or DDoS assault may utilize a significant amount of data, up to a pace of several gigabits per second. DDoS assaults often include the deployment of botnets since many services lack the capacity to defend against an assault from thousands or even hundreds of thousands of infected devices.

DoS Attack used for Profit

There have been many instances of DoS attacks being conducted with malicious intent against users, services, or simply for sheer fun. Services that are under assault may experience slowdowns or crashes for a few hours to many days. The forced downtime for many firms may cause serious user inconvenience or even financial losses. When a service is under assault, users often notice that it either loads slowly, keeps disconnecting, or cannot connect at all. DoS assaults that were undertaken out of business or political rivalry have also occurred in several instances. The 2007 assaults on Estonia, in which many of the internet resources of the Estonian government were attacked, were perhaps the most significant instance of an attack that was associated with political rivalry.

Defending against a DoS attack

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

It used to take a certain amount of technical expertise to launch a DoS assault. This tended to restrict their usage to those who had the appropriate abilities or could discover and employ someone who did. But nowadays, even a novice user may conduct a DoS assault thanks to the availability of simple programs or tools for purchase in criminal forums online. This has greatly increased the likelihood that thieves and other parties intending to disrupt an internet service may carry out such assaults. Many important internet services have adopted different ways for managing enormous floods of data or traffic as a result of the possibility of becoming the target of DoS attacks. Among the anti-DoS strategies are [2]:

i. Jamming

Jamming technology may be highly sophisticated, particularly in many armed units. Electronic warfare (EW) is the broad term for this group of technologies. EW systems may be used to jam a wide range of electromagnetic spectrum-based technologies, including radio, radar, sonar, infrared, laser, and a number of others. Although these technologies are exceedingly costly and sophisticated, they are widely used by military. On the opposite end of the spectrum, jamming is likewise a pretty straightforward process. Plans for specially designed home-made jamming apparatus may be accessible online. Radio equipment can often be modified to obstruct transmission and reception on other devices. Additionally, equipment that operates in the approximate vicinity of the frequency that will be interfered with, such as microwaves and portable phones, may often be employed to some degree. The systems themselves may be targeted since the majority of these systems rely on computers. This is an illustration of denial of service, as used in the online environment [3].

ii. Defense Against Conventional Attacks

There are two key areas where we may deploy our defenses when trying to protect against assaults in the physical and electromagnetic realms: hardening the buildings and equipment against anticipated attacks, and creating redundant infrastructures. By doing this, we may potentially lessen the impacts of any assault that does reach us and try to avoid it from having an influence on us in the first place [4].

A Denial-of-Service (DoS) attack aims to bring down a computer system or network such that its intended users are unable to access it. DoS attacks do this by providing the victim an excessive amount of traffic or information that causes a crash. Both times, the DoS attack denies the service or resource that legitimate users such as workers, members, or account holders anticipated. DoS assaults often target the web servers of well-known corporations, including media, financial, and commercial enterprises, as well as governmental and commercial organizations. DoS attacks may cost the victim a lot of time and money to cope with, even while they normally do not lead to the theft or loss of important information or other assets. DoS attacks typically use one of two approaches: flooding services or crashing services. Flood assaults happen when the server cannot handle the amount of traffic coming into the system, which causes it to sluggishly and finally cease. A common flood assault is:

i. **Buffer overflow attacks:** The most typical DoS assault. The idea is to transmit more traffic to a network address than the system's design allows for. It comprises the following attacks in addition to those that aim to take advantage of flaws unique to certain networks or applications.
ii. **ICMP flood:** Uses faulty network hardware to ping every computer on the targeted network rather than just one particular machine by delivering fake packets. The traffic is subsequently amplified by the network. The scurf assault and the ping of death are some names for this attack.
iii. **SYN flood:** Makes a connection request but never completes the handshake with the server. continues until all open ports are fully used by requests and none are accessible to authorized users.

Other DoS attacks just take use of flaws that result in the target system or service crashing. In these attacks, input is received that exploits flaws in the target and causes the system to crash or become very unstable, making it impossible to access or utilize the system. The Distributed Denial of Service (DDoS) assault is another sort of DoS attack. When several systems coordinate a synchronized DoS assault on a single target, the result is a DDoS attack. The main distinction is that the victim is assaulted simultaneously from several places rather than just one. The spread of hosts that constitutes a DDoS offers the attacker a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

number of benefits [5]:

i. He can launch a severely disruptive assault by using the more powerful computer.
ii. The random dispersion of attacking systems (sometimes global) makes it impossible to pinpoint the attack's site.
iii. Shutting down numerous computers is more complicated than just one.
iv. The genuine attacker is difficult to spot since they hide behind several (usually compromised) systems.

Although most types of DoS assaults can be defended against by modern security technology, DDoS is nevertheless seen as a particularly serious danger and is of more concern to organizations that worry about being the victim of one.

Types of Denial-of-Service Attacks

There are three main types of DoS attacks:

i. Application-layer Flood

In this kind of attack, the attacker just bombards the service with requests from a fake IP address in an effort to slow it down or bring it down, as seen in. Millions of requests per second or a small number of requests to a service that uses a lot of resources might represent this. The service would eventually run out of resources and stop responding to queries. Application-layer DoS attacks may be challenging to defend against. As shown in Figure 1, outsourcing pattern recognition and IP filtering to a third party is the best method to lessen the impact of these sorts of assaults.

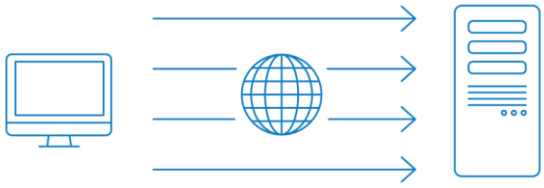

Figure 1: Illustrated the Application Layer Flood

ii. Distributed Denial of Service Attacks (DDoS)

Similar to DoS attacks, distributed denial of service (DDoS) assaults sends out requests from several clients as opposed to only one, as seen in. DDoS assaults sometimes include a large number of "zombie" computers, or devices that have been hacked and are under the control of attackers. Then, these "zombie" computers flood a service with requests to shut it down. DDoS assaults are notoriously difficult to mitigate, hence it is advised to outsource network filtering to a third party [6], [7].

iii. Unintended Denial of Service Attacks

DoS attacks are not always malicious. The "unintended" Denial of Service attack is the third assault type. "The Slashdot Effect opens new window" is the classic illustration of an accidental DDoS. Anyone may upload news items and links to other websites to the internet news portal Slashdot. Millions of individuals may visit the site as a result of a related story's popularity, overwhelming it with requests. The extra traffic may cause the connected site to slow down or even crash if it wasn't designed to manage that type of pressure. Another great example of an inadvertent DoS is Reddit and "The Reddit Hug of Death (opens new window)".

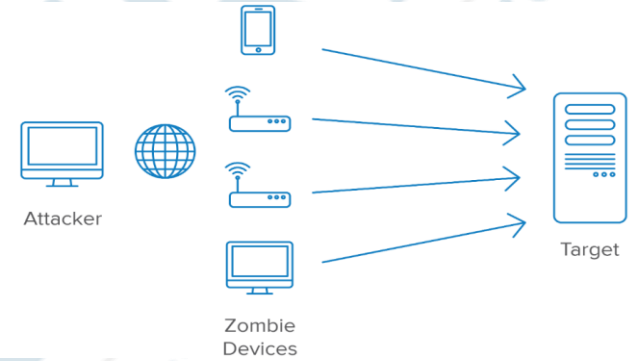

Figure 2: Illustrated the Unintended Denial of Service Attacks

Architecting your application for scalability is the only way to avoid these kinds of unintentional DoS assaults. To prevent your website from going down even when you have high burst traffic, use techniques such as edge caching using CDNs, HTTP caching headers, auto-scaling groups, and others. When providing service to low bandwidth places, another sort of unintended DoS attack could take place. For example, when streaming material abroad, individuals in certain regions of the globe with sluggish or unreliable internet connections may create issues. Packets are dropped when your service tries to transfer data to certain places with limited bandwidth. Your service will try to resend any lost packets to deliver the information to the intended recipient. If the connection loses the packets once again, your service could try again. This cycle may increase the strain on your

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

service by two or three times, making it sluggish or impossible for anybody to access [8].

System Vulnerability and Denial of Service Attacks

Attacks on information networks often start with the identification of a system weakness by skilled hackers. The initial assaults are sparked by the creation and distribution of crude exploit tools. Next, more complex and numerous assaults are launched using cutting-edge automated scanning and exploit tools. On the 'victims' side, a defense-building procedure (identification of the vulnerability's source, creation of a software patch, dissemination, and installation of the patch) follows. The assault wave eventually stops. A "vulnerability exploit cycle" or "vulnerability life cycle" is the term used to describe the whole procedure. Historically, the majority of assaults against information networks have been carried out by the hacker community. Although unpleasant enough, cyber assaults have mostly led to temporary issues. However, when more sophisticated attack tools are created and an exponentially rising number of poorly maintained units owned by lone persons increase the number of susceptible locations to unprecedented levels, the hacker threat might become an increasing annoyance.

DISCUSSION

A DDoS assault affects a target in the same way that a DoS attack does. They vary in that a DDoS assault comes from a number of Internet-connected devices, while a DoS attack comes from a single system. DoS assaults share many of the same techniques as distributed denial of service attacks, but DDoS attacks are more sophisticated and have the ability to cause more extensive harm. DDoS assaults are compared by Bruce Schneider to a pizza delivery attack: Because Alice dislikes Bob, she makes a hundred calls to pizza delivery services and orders a pie from each one to be delivered to Bob's residence at 11 p.m. At eleven, every pizza shop is demanding payment. They are the ones being attacked, and the assailant is nowhere to be seen. The first publicly reported DDoS attack took place in 2000 when hacker "Mafia boy" launched an assault using tools that were readily available online. Among the companies affected by the aftermath were Yahoo, CNN, Amazon, eBay, and eTrade. According to the FBI, it took around 50 computers to bring Yahoo down. This does not imply that the hacker is knowledgeable or that the tools utilized are advanced [9], [10].

CONCLUSION

Denial-of-service attacks aim to stop authorized users from utilizing a service rather than gaining access to computers or data. A denial-of-service attack may take many different forms, but its fundamental goal is to slow down a system by overloading it with information that it cannot handle rapidly enough. The word "malicious code" refers generally to programs that, when run, may have unintended effects on a system. Most of the time, users of the system are unaware of the program until they notice harm. Viruses, worms, and Trojan horses are examples of malicious programming. Trojan horses and viruses are often concealed in trustworthy programs or files that attackers have modified to perform unexpected tasks. Worms are self-replicating programs that propagate once they are launched without the assistance of a person. Although viruses are self-replicating programs as well, they often need human interaction to propagate to other programs or systems.

REFERENCES

[1] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2909807.

[2] M. Basnet and M. H. Ali, “Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning,” IET Gener. Transm. Distrib., 2021, doi: 10.1049/gtd2.12275.

[3] B. L. Chen et al., “The power of Choice : From Standard NFC to Secure Solutions,” 2013 Fourth Int. Conf. Comput. Geospatial Res. Appl., 2014, doi: 10.1017/CBO9781107415324.004.

[4] S. Ismail, E. Sitnikova, and J. Slay, “SCADA Systems Cyber Security for Critical Infrastructures,” Int. J. Cyber Warf. Terror., 2016, doi: 10.4018/ijcwt.2016070107.

[5] M. Basnet, S. Poudyal, M. H. Ali, and D. Dasgupta, “Ransomware detection using deep learning in the SCADA system of electric vehicle charging station,” 2021. doi: 10.1109/ISGTLatinAmerica52371.2021.9543031.

[6] W. Gao, T. Morris, B. Reaves, and D. Richey, “On SCADA control system command and response injection and intrusion detection,” 2010. doi: 10.1109/ecrime.2010.5706699.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

[7] W. Gao, "Cyberthreats, attacks and intrusion detection in supervisory control and data acquisition networks," Mississippi State Univ., 2013.

[8] A. O. Gomez Rivera and D. K. Tosh, "Towards security and privacy of SCADA systems through decentralized architecture," 2019. doi: 10.1109/CSCI49370.2019.00230.

[9] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenco, and T. Cruz, "ELEGANT: Security of Critical Infrastructures with Digital Twins," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3100708.

[10] R. Taormina, S. Galelli, H. C. Douglas, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Modeling cyber-physical attacks on water networks with epanetCPA," 2018.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Analysis of Computer Network Exploitation and Procedures Information

Ms. Manjula Hebbal
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-manjulahm@presidencyuniversity.in

Abstract: ***enabling computer network operations and intelligence-gathering capabilities used to gain information from the target or enemy information systems or networks. Theft of money or financial information, such as bank account information or credit card numbers. The trading disruption results in lost sales or contracts due to the inability to complete transactions electronically. Active and passive assaults on networks are the two primary categories. In passive network assaults, malevolent actors watch and steal sensitive data from networks without making any changes. Data modification, encryption, or damage are all aspects of active network assaults.***

Keywords: Computer Network, Cyber Attack, Ethical Hacking, Internet Security, World Wide Web.

INTRODUCTION

In terms of cyber security, tactics, techniques, and procedures (TTPs) refer to the actions, plans, and techniques that hackers employ to create and carry out cyberattacks on business networks. In essence, TTPs enable security practitioners better protect themselves against various sorts of assaults by educating them on the "why" and "how" of cyber attacker behavior. Here is a more thorough explanation of the strategies, methods, and processes:

i. Attacker tactics explain the technical goals behind their actions (the "why"). For example, the attacker's objective may be to install harmful software on your devices or to take private information from your network.

ii. ii. Techniques explain how an enemy accomplishes their goals. They are the techniques the attacker use to carry out their assault. For instance, when passwords are obscure or encrypted, an adversary may employ brute force methods to access accounts. Some tactics feature sub-techniques that go into deeper depth about how an enemy employs a certain technique. Referring back to the brute force example, an attacker may attempt to access a target account by guessing the password or by password-cracking, which involves using the credentials of unrelated accounts [1].

iii. iii. assault components, including the tools and techniques attackers employed to plan the assault, are described in full in procedures. It's the particular application the attacker makes to achieve a tactic's objective. For instance, an attacker may employ CrackMapExec, an exploitation tool that can gather information on targeted networks, to carry out the brute force tactics and sub-techniques discussed before.

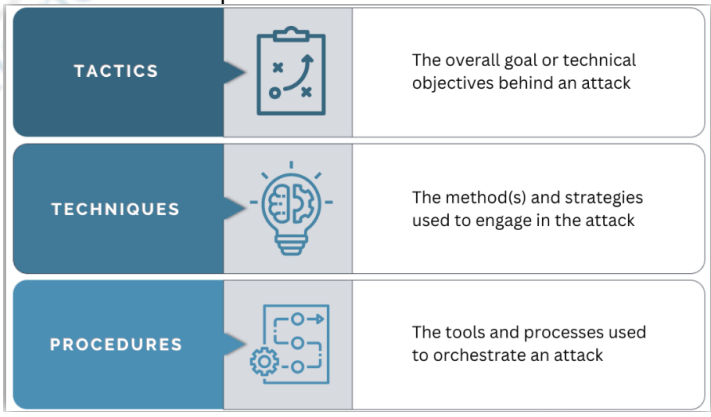

Figure 1: Illustrated the Computer Network Exploitation

The phrase Computer Network Exploitation (CNE),

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

which has military roots and is used in cyberwarfare, could seem a little strange to those who are unfamiliar with the idea. Contrary to what we would be tempted to believe, the term "exploit" in CNE does not relate to exploits employed against systems to get access to them or to remote shells on them. Actually, the term "exploit" here refers to the capacity to use the data or information obtained about our target for personal gain. As stated in the definition provided by the government, CNE is "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks." These activities are the digital version of traditional espionage. CNE is the stage of cyberwarfare that the world is now going through. Although cyber reconnaissance and surveillance operations are often seen, direct cyberattacks between nation-states are still uncommon.

Intelligence and Counter-Intelligence

It might be a little challenging to pinpoint the enemy's identity for CNE reasons. When we refer to an adversary or opponent in the virtual world, we may really be referring to what are actually the second or third order repercussions of our opponent's actual behavior, or perhaps beyond. In other words, it's crucial to know that even if a Distributed Denial of Service (DDoS) assault seems to be originating from a lot of computers in China, the Chinese may just be involved in the attack as an endpoint. We must examine the targets, sources, attackers, and supporters of the activity we are watching in order to really identify the adversary [2].

Reconnaissance

Open-Source Intelligence (OSINT), passive reconnaissance, and Advanced Persistent Threat (APT) are the three main divisions of cyber reconnaissance. Although these three techniques for reconnaissance are mostly at odds with one another, they are all useful in cyber warfare. In many cases, we will want to start by using OSINT to learn as much as we can without explicitly stating our interest, then go on to passive reconnaissance when we need to learn more precise information that we were unable to get via the passive method.

Open-Source Intelligence

In order to keep our target unaware that they are being watched, OSINT entails the employment of techniques. As long as we are cautious not to reveal our objectives while doing them, investigating DNS information, Google hacking, information acquired from websites, investigating document metadata, and other similar techniques may all be effective ways to carry out OSINT operations. We'll probably start with public information when obtaining OSINT, then go on to information relating to jobs, Google hacking, DNS information, and metadata collection. We often start with OSINT while doing reconnaissance on a target before switching to passive. We will primarily want to employ information sources that do not leak information about our interests, or at least minimize such leaking, while using an OSINT strategy to reconnaissance. For instance, the administrators of such an application might find it interesting that the IP address block of a well-known government contract organization suddenly showed a high level of interest in the DNS information of systems connected to the Chinese government, even though we might use a public web-based query tool to conduct research against a target.

In these circumstances, it is often desirable to disperse such requests among several sources and employ a network masking solution like The Onion Router (Tor). We can also utilize a few network monitoring methods for OSINT in a limited capacity. There are packet sniffing tools that are fully passive in nature and are extremely hard to detect without taking particular means to do so, however we are severely constrained in what we can do for sniffing on a wireless network when constrained by the necessity of stealth. There are additional techniques for network sniffing tools that operate by induction rather than a direct interface with the network and are, in principle, physically impossible to detect. Even fiber optic connections, which are often thought too not be passively trappable, are. There are inexpensive tools available to measure the light leakage through a fiber cable's jacket without actually cutting it to put a tap [3], [4].

Additionally, we can eavesdrop on wireless network traffic in relative safety, as long as we are careful not to interact with the network itself. Even encrypted wireless traffic can reveal information about the devices that are connecting to it and, based off of names and Media Access Control (MAC) addresses of such devices, we can often infer quite a bit of information about the environment.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Passive Reconnaissance

While OSINT uses more indirect methods to gather information about our target area, passive reconnaissance is more passive when it comes to the actual target. Compromise of a router utilised by the target, followed by the disruption or degradation of other channels to channel packets to the hacked router where we may more easily eavesdrop on the traffic, is an example of an attack that is passive relative to the particular target. In this scenario, we have changed the surroundings to help us with our reconnaissance but have left the target alone.

Many of the tools we mentioned in Chapter 4 that directly interrogate a network or system to learn its specifics or may be custom developed by the attacker will often be used in passive reconnaissance. As we explained, passive reconnaissance is often the next step in OSINT and may be largely dependent on the data acquired during that operation. The defense could mistakenly provide information to our target during passive reconnaissance from the nodes that are engaged in these duties. Passive reconnaissance may vary significantly from penetration testing in cyberwarfare operations in this regard. There are several scanning tools available, including network sniffers for both wired and wireless networks, port scanners, vulnerability research tools, OS system fingerprinting tools, banner capturing tools, and other similar utilities, that may be used for passive reconnaissance. We'll be trying to list the infrastructure components, networks, and systems now in use, evaluate the ports that are open and the services that are using them, identify the operating systems, and evaluate vulnerabilities. This procedure is meant to serve as a broad guideline and is definitely not set in stone. There may be occasions when a series of intriguing facts will get us to a step earlier than another, and there is nothing wrong with changing our strategy in such situations. If we take the time to meticulously record the knowledge learned on the details of our target area, we often find that our future actions or assaults will experience a far larger degree of success. This documentation will make it easier to plan future assaults or conduct more thorough reconnaissance. It will also guarantee that everyone participating in the operation is using the same set of facts. Additionally, it's crucial to update this documentation if new information or environmental changes are discovered [5].

Surveillance

The main distinction between reconnaissance and surveillance is that the former usually means a single observation of a specific area, whilst the latter often suggests a continuous monitoring. Although lengthy use of such tools would increase the probability of being detected, it is true that any of the techniques and tools we have outlined for performing reconnaissance may be used continuously as surveillance tools, and in fact some of them are. Some of the same fundamental methods are still helpful, but they may be modified to eavesdrop on voice and data exchanges for longer periods of time or to emit electromagnetic radiation. The target of monitoring may be someone or something within our country or organization, which is another factor to take into account. These incidents have undoubtedly become more frequent in recent years, partly as a consequence of a number of significant terrorist acts. Governments may often argue for continued monitoring in the face of such actions, sometimes without even engaging the general public. Such initiatives are often carried out under the pretense of preventing terrorism, drug trafficking, and other like problems. Although regulations that govern domestic surveillance are also often in place, these rules are not always strictly adhered to and are sometimes even completely disregarded in the sake of the greater good. Later on in this part, we will go into more detail about some of these topics.

Voice Surveillance

Conducting voice surveillance on earlier analogue voice communication systems physically included plugging a wiretap a device that records audio into the phone line at some point. Even if these jobs are simpler to do overall and from a distance as we adopt newer methods, we nevertheless refer to them by the same name. In digital phone systems, turning on a function that controls the speech traffic for a specific area might enable such monitoring, turning a hitherto laborious operation into a matter of mouse clicks in an administrative tool [6].

Voice over IP (VoIP) traffic has started to make significant strides towards displacing Plain Old Telephone service (POTs) as the industry norm for voice-based communications in recent years. This is really a positive thing for those who want to monitor these talks since VoIP traffic is much simpler to eavesdrop on remotely and may have less intrinsic security depending on the implementation. Having access to the network traffic and using a sniffing

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

device to listen in on unencrypted VoIP conversations is all it takes to listen in on many commercial and consumer services. With the help of a tool like Wireshark or Cain and Abel, which both have a straightforward point-and-click user interface and will play back an audio version of the conversation in a given packet capture file, both sides of a voice conversation can be recorded in this way and easily decoded and played back.

Data Surveillance

Monitoring infrastructure devices that have been put permanently or semi-permanently with the specific intention of listening to the traffic passing over the network or networks in question are often used to monitor data. When conducting surveillance on a smaller scale, as could be the case at a business, this is often done by installing specialized surveillance equipment, like those made by NIKSUN, in strategic locations across the network architecture. These devices enable the capturing of network traffic, which enables subsequent analysis of assaults, application use, communications, and a wide range of network-related activities. When we want to monitor much bigger amounts of data, such as traffic or traffic patterns for a whole country, such methods do not scale effectively, even if they function quite well for small to medium size monitoring. Organizations with such goals generally governments generally deploy their own solutions or hire companies to create solutions especially for them. As more businesses migrate to the cloud, activity in this sector is predicted to increase.

Large Scale Surveillance Programs

We have a number of excellent examples of large-scale surveillance systems from the US government. Echelon was one of the first such initiatives to make speech and data monitoring possible on a wide scale. The United States, Canada, the United Kingdom, Australia, and New Zealand are the signatories to the US-UK Security Agreement, and they run a network for collecting and analyzing signals intelligence. This network is known as Echelon. A large-scale espionage program called Echelon monitors worldwide voice traffic through satellite, phone networks, microwave connections, and even data sources like fax and email. Echelon's initial mission in the 1960s was to keep an eye on communications between the Soviet Union and its allies. Currently, it is thought to be utilized for gathering broad intelligence data as well as monitoring activity more closely related to terrorism and drug trafficking [7].

The US Federal Bureau of Investigation (FBI) launched the Carnivore program in the late 1990s. Carnivore was a device that could filter out and record all traffic to and from a target when it was connected to the Internet Service Provider (ISP) of the target that was meant to be watched. Carnivore could only filter communications based on the sending and receiving locations because it lacked contextual awareness. The Carnivore program was discontinued in 2001 and replaced with commercial alternatives after great public outcry.

The FBI has again attempted widespread data surveillance through Magic Lantern, which was initially made public in 2001. Magic Lantern operated on a somewhat different tenet. The strategy for this application was to utilize a Trojan horse or exploit that was sent over email to create keystroke logging on a remote PC. The target would install and presumably start sending recorded data to a monitoring station after it had successfully run the email attachment containing Magic Lantern. The FBI acknowledged Magic Lantern's existence in 2002 but said it had never been used.

DISCUSSION

Einstein is a modern, governmental-focused program for data monitoring. It started in 2002 as a program to keep an eye on unauthorized traffic and intrusions at the US government's network gateways. It underwent multiple updates and expanded until 2008 when federal agencies except for the Department of Defense (DoD) and a few intelligence agencies were required to utilize it. Despite being mainly designed as a security precaution for US government systems, Einstein also gathers a large quantity of data as it turns these networks inside out. Einstein's primary objective is "to identify and characterize malicious network traffic to enhance cyber security analysis, situational awareness, and security response." An NSA program called Perfect Citizen scans key infrastructure systems and networks for weaknesses in both publicly and privately operated settings. Government contracts have been provided as large incentives to individuals who are prepared to join in the program, even though it is not required. Government oversight of private businesses, such as electricity corporations, has drawn criticism [8]–[10].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

CONCLUSION

In addition to the immediate applications of surveillance data, with enough data, we can also utilize it as a foundation for identifying patterns of behavior among individuals being monitored. For a while now, the US government and perhaps other agencies have been looking for precisely these patterns in phone and data transactions. The US government, more especially the National Security Agency (NSA), has been doing pattern analysis on voice conversations since the terrorist events of September 11, 2001, to identify trends that might foreshadow a terrorist strike. Using such methods, we can deduce that a particular voice traffic pattern, such as a call from a nation known for supporting terrorism to a location in the United States, followed by consecutive calls from the American number to six other numbers, may very well be a sign of unusual activity. Of course, this presupposes knowledge of the phone numbers to keep an eye on for such patterns or highly powerful computational capacity, perhaps beyond what is presently possible.

REFERENCES

[1] R. M. Laurencio, “Optimización energética de la operación de los sistemas de climatización por agua helada en hoteles,” Intel. Artif., 2016, doi: 10.4114/ia.v18i56.1125.

[2] S. Morrissey, iOS Forensic Analysis for iPhone, iPad, and iPod touch. 2010. doi: 10.1007/978-1-4302-3343-5.

[3] T. D. D. Et. al., “An Investigation and Analysis of Cyber Security Information Systems: Latest Trends and Future Suggestion,” Inf. Technol. Ind., 2021, doi: 10.17762/itii.v9i2.372.

[4] E. Stafford et al., “Assessing the Suitability of King Topologies for Interconnection Networks,” IEEE Trans. Parallel Distrib. Syst., 2016, doi: 10.1109/TPDS.2015.2409865.

[5] B. Middleton, Conducting Network Penetration and Espionage in a Global Environment. 2014. doi: 10.1201/b16797.

[6] R. Burton, V. Tymchenko, N. Sundvall, M. Hoang, J. Mozley, and M. Josten, “WordyThief: A Malicious Spammer,” in eCrime Researchers Summit, eCrime, 2020. doi: 10.1109/eCrime51433.2020.9493261.

[7] R. Montero Laurencio, “Energetic optimization of the chilled water systems operation at hotels,” Intel. Artif., 2015, doi: 10.4114/intartif.vol18iss56pp43-46.

[8] H. Tursina Ratu, Nurhaerunnisah, Musahrain, “Pemberdayaan Peserta Didik Sumer Payung Melalui Literasi Sains Terhadap Peningkatan Minat Baca Dan Berpikir Kritis,” Angew. Chemie Int. Ed. 6(11), 951–952., 2020.

[9] M. Burrows and P. Engelke, “What World POST-COVID-19? : Three Scenarios,” Atl. Counc., 2020.

[10] Rahman, “Penerapan Metode Rough Set Dalam Memprediksi Penjualan Perumahan (Studi Kasus Di Pt. Anugerah Pasadena Pekanbaru),” Fak. Tek. Ilmu Komput., 2020.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Introduction to Computer Network Attack

Mr. Rajaghatta Sunil Kumar
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-sunilkumar.rm@presidencyuniversity.in

Abstract: ***The security and integrity of computer networks are seriously threatened by computer network attacks (CNAs) in the linked world of today. CNAs include intentional operations intended to infiltrate, disrupt, or compromise computer networks for a variety of harmful objectives. An overview of CNAs is given in this abstract, along with information on their goals, operating procedures, and probable outcomes. It examines several CNAs, including malware assaults, denial-of-service attacks, and data breaches, illuminating the wide variety of attack strategies used by attackers. The abstract also highlights the need of strong network security mechanisms, such as firewalls, intrusion detection systems, and encryption, to protect against CNAs. Organizations may increase their resilience against these cyberthreats, safeguarding sensitive data, preserving network availability, and limiting possible financial and reputational harm, by understanding the nature of CNAs and putting appropriate security procedures into place.***

Keywords: Computer Architecture, Computer Network, Cyber Attack, File Transfer Protocol, Internet Security.

INTRODUCTION

The military uses the phrase "computer network attack" (CNA) to refer to "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." We must realise that there is a significant distinction between such acts carried out by country states and non-nation states, even if this word fits well with the prevalent perception of basements full of hackers waging cyber war against the adversary or of lone attackers engaging in similar activities.

It is unquestionably true that, in the context of solely cyber combat, tiny groups or lone attackers may be able to use comparable weapons to a comparable degree of success as a nation-state, but the similarities often stop there. A lone hacker with access to a sizable botnet's command and control system can undoubtedly cause havoc, but those with significantly more resources are frequently the ones who can carry out conventional attacks or use cyberattacks as a support or complement to other attacks. An attempt to disrupt, disable, damage, or maliciously manipulate a computer environment or infrastructure via the use of cyberspace; to compromise the integrity of the data; or to steal information that is under control. Active and passive assaults on networks are the two primary categories. In passive network assaults, malevolent actors watch and steal sensitive data from networks without making any changes. Data modification, encryption, or damage are all aspects of active network assaults.

Differentiating CNA from the attacks we regularly see in the daily attacks from black hat hackers, cybercriminals, and other similar groups that are not being actively sponsored by a nation state, or even in the attacks that we carry out against ourselves in the penetration testing process, is another issue that frequently causes confusion when discussing CNA. The extent, purpose sponsorship, and thoroughness of the offensive procedure are the main differences.

Attacks carried out by random hackers and in the name of penetration testing often don't "go for the throat" the way a typical assault could. Many of these attackers strive to weaken the target environment in order to seize control of it, but they do not go beyond what could be necessary or preferred in real conflict in terms of damaging actions. Such actions might result in the complete destruction or disablement of critical infrastructure through a purely cyber-attack in genuine cyber warfare, where we have a presumably greater intent to significantly impact our target, or might be used to disable systems that offer protection against a conventional attack, such as missile tracking systems, to facilitate such an attack [1].

Waging War in the Cyber Era

When considering them separately, cyber warfare capabilities are not just relatively new, but they also alter how conventional combat is conducted. Any of the existing forms of warfare have additional dimensions when we consider the use of cyberspace.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

The physical, technological, and intellectual aspects of combat must be taken into account in cyber warfare, along with human motivations and the passage of time.

Physical Warfare

Cyberwarfare has a significant influence on how physical conflict is fought. These objects are susceptible to cyber-attacks since even simply physical combat, as in troops on the ground, relies heavily on technology. Support for physical operations relies on a variety of elements, including the timely delivery of supplies, the efficient movement of troops, the efficiency of communications, and many more. Our exclusively physical combat may swiftly descend into chaos if one or more of these acts are not carried out or, even worse, are changed to engineer a vulnerability. for the other hand, physical interference may have a significant negative impact for cyberwarfare operations. Our relatively delicate computer systems and infrastructure become useless if communications are disrupted, electricity is cut off, environmental conditions are not maintained, or any other number of requirements cannot be satisfied [2]. In either scenario, cyber warfare assaults may influence or be influenced by physical combat. We may miss a significant chunk of the overall picture in cyber warfare when the physical element is disregarded. Although cyber warfare is a separate kind of warfare, separating it from other types of warfare just makes its capabilities, at best, insufficient.

Electronic Warfare

Electronic warfare, while sometimes seen as a subset of conventional or physical warfare, may have a significant impact on cyberwarfare, and vice versa. The systems that are used to conduct cyber warfare heavily rely on this region, from which they are particularly vulnerable to disturbance, and electronic warfare is primarily concerned with assaults that take place there (think analog vs. digital). Without striking a single physical blow, we may be able to disable the infrastructure and systems that make up our adversaries' cyber warfare capabilities by using electronic warfare methods.

Similarly, the systems that enable electronic warfare are often of a highly technical type and might be vulnerable to cyberattacks. One may imagine a scenario where a nation-state would try to use electronic warfare to disable an opponent's cyber capabilities only to discover that a cyberattack has rendered its electronic warfare useless.

Logical Warfare

We also need to take into account assaults that are only focused on computers at the beginning of this section. As we covered previously in this chapter, such assaults may be used for espionage and monitoring, but they can also be used to launch direct attacks against other systems and infrastructure. These types of assaults make up the bulk of CNAs, and we will spend a lot of time talking about them in the assaults section later in this chapter [3].

Attacks that are just rational lack a great deal of potential to be successful in a larger military effort. Although it is quite simple for almost any party to acquire and use such weapons to great effect, the inability to launch further assaults is immensely restricting. If we take conventional battles as an example, waging cyber warfare without air support may be comparable to conducting conventional warfare without the use of air support; it is undoubtedly conceivable, but severely constrained.

Reactive vs Proactive Attacks

When thinking about cyberwarfare assaults, we have the option of acting reactively, either by defending against an attack or by reacting to our adversaries' activities. We may also take proactive action by foreseeing actions that result from threats or actions taken by our adversaries that seem to be a step toward an unfavorable situation. We can use tactics that are not immediately detrimental or outwardly destructive and do not need the actual deployment of soldiers or resources to carry out such actions, thanks to cyber capabilities.

We'll probably keep using the paradigm of conventional combat when we react defensively. Even while we don't necessarily need to transfer resources there, we still need to carry out many of the staging procedures needed to prepare for a fight of this kind. Most likely, this will include carrying out many of the reconnaissance tasks that we covered in this chapter's section on computer network exploitation (CNE), and it could even be possible to take advantage of any continuous monitoring that was already in place against our target. We may then go on to CNA after such efforts are finished to the point where we have enough knowledge to launch assaults.

We have a very wide range of warfare options available for use, up to and including an all-out assault, if we are to conduct cyber warfare proactively. Attacks that are planned ahead of time but aren't launched until the circumstances are optimal and opportune for us to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

do so have a lot of potential use. Such logic bomb strategies may be planned out years in advance and may even infiltrate our adversary's hardware. In Chapter 6, in the section titled "Supply Chain Concerns," we went into additional detail about these actions. When this occurs, preemptive action that has been meticulously prepared may be employed to completely leave the adversary helpless just when they are most reliant on their equipment and weapons to do their jobs [4].

The Attack Process

Typically, the assault procedure is concentrated on a specific system or group of systems. In this procedure, as seen in Figure 1, we'll probably carry out more extensive reconnaissance and scanning to get even more precise information from the system. As our requirement for secrecy and stealth may not be as high as it was when we were conducting CNE, we may be able to perform reconnaissance in more detail at this level. Then, either by an open attack or by utilizing credentials we have managed to get someplace in the environment, through social engineering, or by employing other methods, we will try to enter the system. Once we've created an account on the system, we may need to increase our degree of access in order to achieve our objectives. Such privilege escalation often targets root or administrator level access, allowing us a certain amount of flexibility inside the system. Once we have the required degree of access to the system, we are free to exalt whatever information we want, harm the environment whenever it serves our interests, and put in place any safeguards we see necessary to guarantee access in the future.

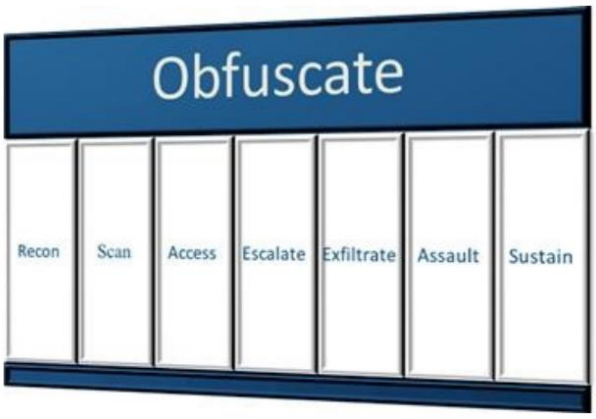

Figure 1: Represented the Different Types of Attack Processes.

Attack Process

The attacker will also try to conceal or obscure their actions at every stage of the assault. To prevent their attacks from being linked to them, they could wish to act as if they are attacking from a different place than where they are, or they might take other actions. When the attacker leaves the system, they probably want to erase any evidence of their actions. This deletion of logs or forensic evidence may benefit from the knowledge gained by current hackers and criminal activity.

Recon

Earlier in this chapter, we spent a significant amount of time talking about reconnaissance and surveillance in the context of CNE. In such a situation, the reconnaissance we would do would be done broadly to map out and learn details about our target area. Given our possible enhanced degree of access and less requirement for stealth, we will most likely already have such generic information from the CNE phase while doing reconnaissance in the context of CNA and the assault process. Instead, we will be looking for information on a much more granular level [5], [6].

Social engineering is a further resource that could be helpful during this more focused phase of reconnaissance. We may very well be able to access the systems in issue without having to use the entire range of assaults that we may otherwise require by using some of the social engineering techniques that we will examine in Chapter 6. Through social engineering, we may be able to identify shared passwords for other services or apps, obtain account names by snooping about the physical spaces of people who work there, go skip diving or utilize any number of other similar techniques.

We could also wish to install the tools that would enable such monitoring on a specific system given the goal of long-term reconnaissance at a more detailed level. Although just a very tiny part of the data produced by software like a keyboard logger will typically be of tremendous use, even on this scale, it could still be well the effort. We often uncover passwords that are manually synchronized across several systems, which is a big help when trying to get access, particularly in circumstances where proper password hygiene is not tightly enforced with technological safeguards. If less secure methods like telnet, File Transfer Protocol (FTP), or Post Office Protocol (POP) are permitted in the environment, we could also be able to sniff credentials from network

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

traffic. Reconnaissance is a broad term that refers to a multitude of tasks that rely greatly on the area in which they are performed.

Scan

Instead of doing the same broad port scans, fingerprinting, service versioning, and other tasks that we did in our general reconnaissance, we will probably be looking much more deeply at the system for possible vulnerabilities during the scanning section of CNA. In general, we will be looking for more precise information from the operating system itself as well as further comprehensive information from apps.

We often concentrate on locating an exposed application that may be especially chatty, such as a web interface to a database, and focus on digging down from there when trying to get more information from apps than simple checks for programs and their versions. This is often a manual procedure that takes time but may be highly beneficial. By using this technique, we can often get highly precise information, such as database versions from error messages, probable usernames from running SQL injection attacks via the web interface, and a variety of other tidbits.

We could also wish to gather further details about the operating system, such as details about individual patches applied, uptime, or any of the other data that would enable us to draw conclusions. When we reach the attack and escalation stages of our process, these extra little facts may help us in our attacks. Documenting this information properly may be extremely beneficial throughout the process, as we covered in the more basic information collecting parts of the first half of this chapter [7].

Access

Several tools and techniques may be used to get access to a system. We may very well have legitimate credentials with which we can easily log in if we have previously been successful at social engineering, skip diving, stealing or cloning access cards like Common Access Cards (CACs), or finding accounts with synchronized passwords on other systems. It's a little trickier than that, but more probable that we'll be able to locate usernames on the system and either guess or break passwords using some of the techniques we covered in Chapter 4 to get access to them.

We might also utilize client-side assaults against certain systems that belong to the users of our target system to acquire quick access. Such attacks use a web browser or other client-side software vulnerability as an attack vector. As opposed to trying to get access to a well-maintained and patched server, we have a far better chance of being able to access specific workstations to obtain credentials. Client-side attacks may be carried out over the web, by email, via a USB stick, or by a variety of other means. Such assaults have a high degree of success, especially in non-technical working situations, while we may not find as much success in fully guarded workplaces.

To get access to a system, we may also try to employ popular operating systems or application vulnerabilities. We have probably previously utilized one or more of the many vulnerabilities scanning tools at some point in the process, either during the more thorough reconnaissance step or during the more focused review throughout the assault process.

DISCUSSION

Privilege escalation, also known as obtaining more or higher-level privileges than those we now possess, may be necessary once we have achieved some degree of access to a particular system. Vertical privilege escalation is the process of seeking to access accounts with a greater degree of privilege than those we currently possess. Horizontal privilege escalation refers to the process of seeking to access accounts that are not currently under our control but are on the same level as the account to which we already have access. Both types of privilege escalation are possible using several techniques. We now have access to the system as a user; therefore, we may be able to employ a different set of vulnerabilities than we used before. We could potentially be able to profit from incorrect or improperly specified setups. It is certainly feasible that, on some systems, the standard user account that we were able to access may immediately assume the role of an administrator or could raise their power level using conventional operating system capabilities [8]–[10].

CONCLUSION

We could also be able to make use of the privileges of programs that are running under more restrictive restrictions. Applications that need privileges beyond those of a regular user, such as backup applications, servers, daemons, or other processes, are often targets for attack. By exploiting various application weaknesses like race situations or buffer overflows, we may run arbitrary code via these already-running apps. We could also be able to access and alter

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

improperly protected interpreted scripts or shell scripts, which would allow us to directly access an operating system shell or transmit operating system instructions via them.

REFERENCES

[1] L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race, "Tennison: A distributed SDN framework for scalable network security," IEEE J. Sel. Areas Commun., 2018, doi: 10.1109/JSAC.2018.2871313.

[2] H. Hou et al., "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2983953.

[3] M. S. Barik, A. Sengupta, and C. Mazumdar, "Attack graph generation and analysis techniques," Defence Science Journal. 2016. doi: 10.14429/dsj.66.10795.

[4] A. Kotkar, A. Nalawade, S. Gawas, and A. Patwardhan, "Network Attacks and Their Countermeasures," ISSN Int. J. Innov. Res. Comput. Commun. Eng., 2013.

[5] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," Sustain. Cities Soc., 2020, doi: 10.1016/j.scs.2019.101728.

[6] H. Kwon and J. Lee, "Diversity adversarial training against adversarial attack on deep neural networks," Symmetry (Basel)., 2021, doi: 10.3390/sym13030428.

[7] W. Alhakami, A. Alharbi, S. Bourouis, R. Alroobaea, and N. Bouguila, "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection," IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2912115.

[8] H. J. Highland, "Security in computing," Comput. Secur., 1997, doi: 10.1016/s0167-4048(97)90261-3.

[9] S. D. Fried, "Penetration testing," in Information Security Management Handbook, Sixth Edition, 2007. doi: 10.32014/2018.2518-1467.25.

[10] A. D. Joseph, B. Nelson, B. Nelson, and J. D. Tygar, Adversarial machine learning. 2019. doi: 10.1017/9781107338548.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of Psychological Weapons

Mr. Mohammed Mujeerulla
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-mohammedmujeerulla@presidencyuniversity.in

ABSTRACT: ***That evaluation is used by cyber defense teams to forecast a hacker's anticipated abilities and the types of risks they would be ready to take, he said. To comprehend why these individuals is doing the way that they are and what drives them, you must simultaneously practice psychology. Because of it, they may plan their next move. He emphasized that it may be difficult to identify an ego-driven hack, for instance. Tools that foretell unusual behavior on a specific machine might be useful. According to Chris Steed, chief investment officer at Paladin Capital Group, a venture capital company that invests in cybersecurity providers, a small but rising number of technology businesses provide tools that mirror certain results from cyberpsychology.***

KEYWORDS: ***Cyber Attacks, Computer Systems, Human Intelligence, Internet Security, Phycological Attacks.***

INTRODUCTION

In chapters four and five, we discussed technological assaults; in this chapter, we'll concentrate on utilizing the target's actions to obtain their information. To affect foreign audiences' emotions, motivations, and rational thinking and ultimately, the behavior of foreign governments, organizations, groups, and individuals' psychological operations (PSY OPS) are planned activities. For ages, militaries have engaged in PSY OPS or influence operations. Army Special Forces (Green Berets) were established by the United States to use persuasion rather than brute force to win battles. Human Intelligence (HUMINT) gatherers and intelligence services use comparable strategies to persuade hostile individuals to spy for their nations. Con artists who are skilled at winning someone over to their benefit have utilized similar methods throughout civilized culture. Salespeople use a variety of techniques to persuade customers to buy the costliest automobile. Now, these methods are being adopted by hackers and cyber warriors to persuade people to disregard rules and common sense so they may access crucial data. This practice is known as social engineering [1].

Social Engineering Explained

Social engineering (SE) is the practice of persuading someone by playing on their emotions or by winning and losing their trust to obtain access to their system. This may be accomplished in a multitude of ways, including in person, over the phone, by email, on social media, and more. As opposed to other types of assaults, social engineering uses human beings as attack vectors, or "wetware" in hacker parlance.

An SE attack seeks to establish a rapport with its victims, earn their confidence, and persuade them to do something or divulge information that is against the rules of their organizations or their fundamental security procedures. Some people can charm others and can do it over the phone, but the majority of attackers will take the time to craft a tale based on facts they already know about the victim. This assault method has developed quickly over the last few years and is now the approach of choice for select targets.

Social Engineering science

How does the science of social engineering work? Recent kinesics (the study of body and facial expressions) publications include Marvin Karlins and Joe Navarro's "What Every Body Is Saying: An EX-FBI Agent's Guide to Speed Reading People" and Paul Ekman's works on micro facial expressions. With the help of books like "Emotional Intelligence: Why It Can Matter More Than IQ" by Daniel Goleman and "Blink: The Power of Thinking Without Thinking" by Malcolm Gladwell, which discuss how intuition is based on insights a person may not be consciously aware of, a body of knowledge that can be applied as a science rather than an art begins to develop. These investigations are creating the foundation needed to transform this field from an art to a science.

In light of this, the question "Can SE be taught, or is it a natural ability?" arises. There is considerable disagreement about whether SE talents can be taught,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

but this disagreement is essentially the same as that over whether leadership, salesmanship, or any other similar skill can be taught. Even while the debates are often quite heated, most individuals will eventually come to the same conclusion: although some people may study and practise in the field they wish to master and still only become mediocre, others can go through the same process. Therefore, although some people may naturally become highly skilled at technical hacking, they may struggle to employ social engineering tactics like the "cold call," everyone can master the fundamentals and identify their area of expertise. Many of the strategies, approaches, and methods we'll cover combine technical and SE assaults [2].

SE Tactics Techniques and Procedures (TTPs)

The target determines the usual SE exploit. The two main situations are broad targeted access assaults and universal access attacks. If we were told to take a vehicle in the next week, it would be simple, but most analogies when used to cyberspace are harmful since they don't represent the complexity of the environment. In a general access attack, we could wait outside a convenience store for someone to leave their car running, get in, and drive off, making sure to check for a child seat, or we could use a gun to carjack someone at a stoplight, learn how to hotwire a car, or use any number of other methods. A different tale would emerge if we had been instructed to target a particular automobile to take from the Commanding General. We didn't need to do any reconnaissance in the first scenario, but we now need to work very hard on it. To devise the most effective defense, we must determine what motivates them. Given that the mayor has power over the police, we need to know which assault has the lowest likelihood of being discovered. Depending on our goals, we could prefer that the theft go unreported for a while or that it be sensational enough to make the evening news. The same principle applies to cyberattacks, but since SE involves some kind of interpersonal contact, it is much more important to comprehend the target.

Let's start with generic assaults. The objective of these assaults is to break into any system or network. The owner of the system means nothing to the attacker. An example would be a broad phishing assault. There are 183 billion spam emails sent daily, and 2.3% of them are phishing scams, therefore sending emails is inexpensive. These systems may be used to attack other systems or be attacked themselves. The construction of systems between the attacker and the targets may be accomplished by harvesting a large number of systems. Reconnaissance is not necessary since the attacker doesn't care where the system is or what it does; they may just launch an attack and, given the minimal expenses involved, accept the smaller number of compromised systems. Therefore, using this SE-based method would be a wonderful way to create a botnet army.

The introduction of a targeted virus, which exclusively targets certain notations in military systems, is the following illustration of a general assault. A virus is a corrupted program that the user must execute in order for it to function. A virus may be loaded by an attacker into a word document, PDF, power point presentation, image, or even a game. These infected files can be opened and operated; thus someone might launch a power point presentation and browse the slides as the virus spreads across the machine. An assault like this might grow viral and wind-up infecting systems it was not meant to target, which is a drawback. A worm, which is a malicious program that doesn't need human input and infects a system before using it to infect others, may also be used in this form of assault. However, this would not be considered a SE attack; rather, it would be classified as a technical attack. This kind of assault has become considerably simpler because to the abundance of translation websites on the internet and the simplicity of accessing intriguing news from the targets' native country. creating plausible narratives with appropriate language and cultural background that often persuade prospective victims to fall into the trap [3].

Standard types of attacks generally designed to steal identities:

i. **Phishing:** Here, an email is sent in bulk to a huge number of addresses (perhaps millions). If the computer system in issue was susceptible, any of these activities would result in the system being compromised: the email may attempt to persuade the user to open an attachment or visit a website.

ii. **Pharming:** Misdirecting users to a fraudulent website.

iii. **Spear Phishing:** This is when a certain person is chosen as the target and a personalized email is sent, which they will open and respond to. Examples include the network's system

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

administrator or a target's program manager. This calls for thorough information gathering about the desired target.

iv. **Whaling:** The targeted organization's high level of leadership is the target of a spear phishing assault.

v. **Smishing:** To persuade the recipient to visit a malicious website or divulge personal information, SMS texts are sent.

vi. **Vishing:** using VoIP to make a call in order to access a system's personal or financial data while the call is being made.

We'll now examine assaults that were specifically targeted. After gathering as much information as they can on the target via what the military refers to as Open-Source Intelligence (OSINT), the attacker will approach the target. People would simply refer to this as "googling" them. The attacker seeks to comprehend the victim's preferences, phobias, drives, attitudes, and aspirations. In doing so, the attacker will be able to customize their assault and raise their chances of success. Important details include knowing important dates (birth, marriage, etc.), addresses, phone numbers, family members, hobbies, connections, photos, and histories of one's employment and schooling. This is a terrific place to start if the target is active on social networking sites; the bigger their electronic footprint, the better. The target may be learned about in a variety of places:

i. Personal info can be found on social media sites like Facebook or Myspace i.e., this includes relationships, activities like sports, volunteering, religious practices, and political beliefs.

ii. Professional info is on networking sites like LinkedIn or job sites like Monster.

iii. Geolocation info on sites like Google Earth or location-based services like Foursquare.

iv. Financial info like tax records and homeownership records.

v. What they are thinking can be read via their Twitter or blogs.

vi. Involvement in virtual worlds like Second Life or gaming site.

vii. Membership info from organizations like academic alumni, clubs, professional organizations, or hobbies.

Exfiltrate

One of our main priorities, once we have the required access to the environment, is to locate any data that would be important to us and exfiltrate it to a place that is accessible to us from another location or to transfer it straight to our systems. Exfiltration is a threat to secrecy and perhaps availability in terms of secrecy, Integrity, and Availability (CIA).

We have a very wide range of tools at our disposal to exfiltrate data, ranging from protocols and tools that are specifically designed for moving data around to more general tools that can be modified for this purpose and even out-of-band techniques that may allow us to bypass security measures intended to specifically thwart such attempt [4].

In straightforward situations, we could be able to transport our files or data with ease using popular tools and protocols. FTP, Secure Copy Protocol (SCP), Extensible Messaging and Presence Protocol (XMPP), and a variety of other popular protocols may all be used to transmit files. These specific transfer protocols may be restricted for outbound traffic in many situations; however, HTTP traffic is often permitted and will work well for our needs. Any situation where we cannot identify some type of outbound protocol on which we may piggyback information is uncommon and very secure.

Assault

The assault phase, which is often left out of the penetration testing process, which, in general, closely resembles our attack procedure, is what distinguishes it from a military operation. In the event of true cyber warfare, it is possible that once we have gained access to a device, advanced to the necessary degree of privilege, and exfiltrated any valuable information, we may wish to exploit the system to create havoc in the surrounding area. In military parlance, the five Ds deception, disruption, denial, degradation, and destruction are used to characterize the effects of such actions. These assaults will primarily target availability and integrity, according to the CIA. Once we have full access to a system, we may want to change its configuration to guarantee that we can access it in the future. When we originally could do so, we may have utilized a particular exploit to get into the system and raise our privileges, but we can't always rely on those avenues of entry being open in the future. To protect against this possibility, we'll probably want

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

to set up new accounts, open services on extra ports, install command and control software, embed backdoors in apps, and other measures.

The efforts that are least evident and least likely to be unintentionally found by a system administrator will probably be the most effective. Particularly on an internet-facing system, some of the more overt techniques, such as creating a new listening port on the machine, may very well be discovered quickly. Furthermore, we may want to be cautious about placing such precautions in locations where another attacker can discover them. Since many of the ready-made backdoors utilize standard ports by default, if we don't modify them, our backdoor can be quite simple to find.

[5].

Obfuscate

Obfuscating is probably the first and final thing we do on a system that we have hacked or plan to breach. Obfuscate means "to bewilder, confuse, or stupefy." This phrase is used by us to refer to both prospective strategies for hiding or erasing proof of our infiltration and for perhaps directing any potential investigators to an altogether another source. Underneath all of the actions we will perform throughout the attack process is a layer of obfuscation. others of these obfuscator acts happen even before our initial recon, others happen throughout our numerous assaults, and some happen just before we leave the system for good.

The simplest and first obfuscation techniques we may use are those that will make it impossible to pinpoint the exact location of our assaults. These tools might be different proxies, like Tor, or intervening computers that we utilize as a connection intermediate before attacking, IP spoofing, or any of a number of other techniques that we can use to hide our place of origination. Even while some of these technologies may not be flawless, they do provide an extra measure of security in case our actions in the target area are discovered.

We'll probably take precautions to make sure we don't leave any digital forensic evidence on the target machine. In these situations, we may adjust timestamps to reflect the time before we made any file modifications, clear up any tools we've added to the system, delete or modify log entries, and generally make sure we haven't unintentionally left any traces behind. We may very well wish to leave such traces behind on the opposite side of the same process, but we will likely change them so that they point to a different source. If we can fraudulently attribute an assault to another source, we may be able to disguise our tracks while also causing a great deal of uncertainty and unrest [6].

Types of SE approaches

The attacker must choose how aggressive they want to be after gathering the background data required to comprehend certain possibilities for approaching the victim. The methods include observation, dialogue, interview, interrogation, and torture, going from least to most forceful. They might begin by being observed physically or digitally. The next step is a discussion, whether it be verbal or written. The attacker will often choose whom to assault or recruit at this stage. This is sometimes referred to as elicitation, which is the process of gathering data via what seems to be a casual discussion. To put it another way, this is the situation when the con or tale relies on the SE's capacity to fabricate information. This skill stems from pretexting, which is the process of creating a situation where the SE earns the confidence of the person who owns or has access to the information in order to persuade them to violate their rules or defy logic and provide the information to the attacker. Mirroring is a technique that is employed in all attacks but is particularly helpful in this situation. It will be much simpler to engage a target in discussion if you emulate their speech mannerism (or email style), for instance.

The next tactic is to interview the subject or directly interrogate them. Both of these call on the victim to accept the attacker's dominance. This may be accomplished by claiming to be a client in need of the knowledge to make a choice, by acting as a government official with access to the information, or by using intimidation. These assaults might be launched immediately or after a connection has been established. The perpetrator may carry them out in person using props like badges or over the phone or email by spoofing the contact to make it seem like it is coming from a reliable source. An example would be to phone the Help Desk and request that they reset the user's account since a recent update went wrong. The majority of individuals instantly trust their computer out of a desire to be helpful. The secret to subverting them is that want to support them or to have faith in their system. These two methods are not inherently in opposition to one another. The most successful strategies often rely on creating ties between people. All of these strategies call on developing a connection based on trust. Torture is the last resort for

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

questioning, but this goes beyond SE procedures. Figure 1 depicts the progression of these strategies [7].

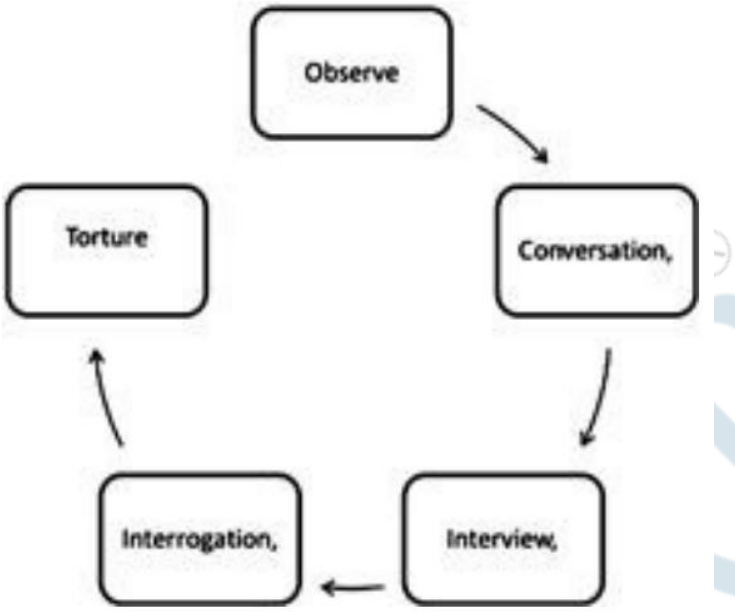

Figure 1: Illustrated the Approach Techniques from Most to Least Aggressive

DISCUSSION

There are physical and electronic types of common collecting procedures. Physical techniques include things like: Dumpster Diving sifting through the target's garbage, Shoulder Surfing while they work, Observation following their movements, like a stakeout, Spy Gear like directional microphones and hidden cameras, and Impersonation pretending to be a utility worker. Open web search, learning to utilize all of your search engine's functions (e.g., Google will only search blogs), Searches on social networking sites, business networking sites, pay-for-service websites like Intaglios or US Search, credit information requests, and geolocation websites like Google Street View [8]–[10].

CONCLUSION

This is just a summary of the many tools that may be used in social engineering, and the list is always changing, therefore look up comparisons to these tools as well. The media recently focused on the SE Capture the Flag competition at DEFCON 18 titled "How Strong Is Your Schmooze." Although a network-based CTF tournament has always been held, in 2010 there was also a SE CTF. An extract from the event report is provided below: Each contestant was given a target organization, and they had two weeks to create a profile using passive information-collecting methods. During this period, no contender or target was permitted to make direct contact. The data was assembled into a dossier, which was submitted and scored as a component of the contestant's overall score. The remaining 25 minutes of DefCon were given to competitors to call their target and gather as many flags as they could, which contributed to their final score. Non-sensitive information was chosen for the flags, and each one was given a point value depending on how hard it was to collect the information linked with it. In-House IT Support, New Hire Process, Anti-Virus Used, Is There A Cafeteria, Wireless On-Site, Badges for Bldg. Access, and What OS Used are a few instances of the 25 flags. The finalists' thorough searches produced several PDFs and online sites that provided comprehensive responses to each of their questions.

REFERENCES

[1] M. R. Kamaluddin, A. Othman, K. H. Ismail, and G. A. Mat Saat, “Psychological markers underlying murder weapon profile: A quantitative study,” *Malays. J. Pathol.*, 2017.

[2] R. Skopec, “New Psychological Weapons Make Targets Hallucinate,” *Am. J. Biomed. Sci. Res.*,

2019, doi: 10.34297/ajbsr.2019.02.000574.

[3] J. Andress and S. Winterfeld, "Chapter 8 - Psychological Weapons," *Cyber Warf. (Second Ed.*, 2014.

[4] R. Skopec, "New Psychological Weapons Make Targets Hallucinate," *J. Transl. Sci. Res.*, 2020, doi: 10.24966/tsr-6899/100004.

[5] R. L. Trivers, "Parent-offspring conflict," *Integr. Comp. Biol.*, 1974, doi: 10.1093/icb/14.1.249.

[6] C. L. Johnson, P. Wilcox, and S. Peterson, "Stressed Out and Strapped: Examining the Link Between Psychological Difficulties and Student Weapon Carrying and Use," *Crim. Justice Behav.*, 2019, doi: 10.1177/0093854819826110.

[7] D. S. Oliveira, T. Lin, H. Rocha, D. Ellis, S. Dommaraju, H. Yang, D. Weir, S. Marin, and N. C. Ebner, "Empirical analysis of weapons of influence, life domains, and demographic-targeting in modern spam: an age-comparative perspective," *Crime Sci.*, 2019, doi: 10.1186/s40163-019-0098-8.

[8] Mr. Aniruddha Vithal Babar, "Rape as a Continuing Weapon of Psychological Warfare, Suppression & Subjugation," *Int. J. Indian Psychol.*, 2016, doi: 10.25215/0302.142.

[9] A. A. Gostev, "Psychological aspects of global manipulation studying," *Psikholog. Zh.*, 2017, doi: 10.7868/S020595921704002X.

[10] O. P. Nevelska-Hordieieva and V. O. Nechytailo, "MANIPULATION AS A MEANS OF INFORMATION AND PSYCHOLOGICAL INFLUENCE IN THE INFORMATION WAR," *Bull. Yarosl. Mudryi Natl. Law Univ. Ser. Philos. law, Polit. Sci. Sociol.*, 2021, doi: 10.21564/2663-5704.50.235389.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of the Military Approaches Social Engineering

Ms. Thasni Thaha Kutty
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-thasni.t@presidencyuniversity.in

ABSTRACT: ***The method of manipulating, swaying, or duping a victim to take over a computer system or steal sensitive data is known as social engineering. Users are duped into divulging critical information or committing security blunders via psychological manipulation. To attempt to acquire sensitive information, social engineering is one of the most popular tactics used by cybercriminals. To mislead someone into providing them with login credentials, bank information, or other forms of data they may use for their objectives, they may pretend to be a reputable business or person.***

KEYWORDS: Army Doctrine, Cyber Attack, Social Engineering, Software Engineering. World Wide Web.

INTRODUCTION

The military has long been involved in the espionage and counterspy industries, and they are also masters of questioning. While questioning is often employed to get information in urgent circumstances, spying is the long-term con. This section will concentrate on the short-term data collection (or short con) as it pertains specifically to SE. We'll examine information extraction methods and talk about how they relate to SE.

First, it's important to remember that both peacetime activities and war scenarios may benefit from these tactics. They often take place in a controlled setting and are quite similar to the strategies used by law enforcement organizations. The underlying ideas and many of the methods apply to SE assaults, and the basic principles are comparable to SE. Military interrogators get training and education, and the majority pursue careers in the field.

They acquire fluency in the local dialects and cultural practices. Human Intelligence (HUMINT) operators or interrogators are trained to handle vetting refugees, briefing US and allied forces, questioning prisoners of war, interviewing collaborators, utilizing captured information, coordinating with the host nation, providing interpreters as necessary, and interacting with the local populace [1].

Army Doctrine

Since the Army is dealing with these challenges on the ground, we will talk about how they handle questioning. The fundamental methods we'll discuss are from "FM 2-22.3 Human Intelligence Collector Operations September 2006".

Goal: The collector's goal during this phase is to build a rapport with the source so that the source will respond to the HUMINT collector's queries with accurate and trustworthy information.

Key principles: The HUMINT collector must be aware of the following behaviors from a psychological perspective:

i. When under stress, they like to converse and they react well to compassion and understanding.
ii. Be respectful while dealing with higher authorities.
iii. Work within a set of culturally and personally generated principles.
iv. Pay attention to your emotional and, more crucially, bodily self-interest.
v. When faced with an unorganized or unusual scenario, fail to implement or recall security lessons they may have been taught.
vi. Be open to talking about a subject where the HUMINT collector has similar or relevant expertise or knowledge.
vii. Value flattery and absolve them of wrongdoing.
viii. Consider a subject less important if the HUMINT collector treats it often.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

ix. Take offense when someone or something they appreciate is disparaged, particularly when it's done by someone they detest.

The HUMINT collector portrays a believable persona intended to elicit cooperation from the source using these concepts to construct an approach, establish rapport, and create a relationship. Things are often done in the military according to established protocols, and if there's a mission, it should have a plan that's been written down. This is not to mean that they are rigid and resistant to change, but rather that they want to improve the likelihood that their goal will be successful and have discovered that doing so requires having a strategy in place from the beginning. The HUMINT collector must make sure that their approach, body language, and demeanor are consistent.

Direct, incentive, emotive (Love, Hate, Fear, Pride, Futility, and Anger), "we know all" or "file dossier," rapid-fire (don't let them speak), Mutt and Jeff or good cop, bad policeman, and false flag (misrepresentation of oneself) are a few examples of standard operating method approaches. To see how they connect, go to Figure 6.2. The direct approach is easy and uncomplicated. It involves giving the subject what they want and persuading them to comply and divulge the information utilizing interview/interrogation techniques. In a conventional conflict, this tactic is helpful, but it is less effective in counterinsurgencies or social engineering. According to statistics from World War II interrogation operations, the direct method was 90% successful. During Operation Urgent Fury and in Vietnam [2], [3].

DISCUSSION

The effectiveness of the direct approach in Operations Enduring Freedom and Iraqi Freedom is still being studied; however, unofficial studies indicate that in these operations, the direct approach has been dramatically less successful. The military is still analyzing the reasons but one common assumption is that the motivations of religious fanaticism are harder to compromise than traditional nationalism.

The Various Approaches Must be integrated

Some common categories of direct inquiries are helpful: Initial to start the conversation, Topical aimed at determining how much each party will talk and their degree of expertise, Follow-up to ensure that we have gathered all the relevant information, non-pertinent to build rapport and keep the conversation going, repeat to check for consistency, Control to establish a baseline, and prepared for topics the interviewer is unfamiliar with or that are highly technical. The control or baseline question is one of the important ones here. It demonstrates a person's behavior when they are being honest. A SE must comprehend how the target acts when not under stress to assess responses accurately, just as a polygraph test progressively progresses from questions about your name and address to questions about your criminal behavior so they can compare the stress reactions to the baseline.

When we combine information collecting with regular interactions with our targets of interest while they are unaware that they are being questioned, the indirect technique, also known as employing elicitation, may often be helpful. When more traditional collecting methods are ineffective, complex elicitation techniques are utilized. This is the least apparent collecting technique, out of all of them. It is crucial to keep in mind that elicitation is a deliberate, methodical procedure that needs careful planning. Here, the interviewer's knowledge of the target is key to facilitating a dialogue that flows naturally. To make the target believe they are fully informed and willing to share the facts, they can, for instance, begin by offering knowledge they already possess. You may accomplish this in person or online using social media. The next step is an incentive, which is essentially giving the target something they need or desire. Bribing someone is the first thing that springs to mind, but it may be as easy as sending them an email with an offer to improve their speed or access to the internet. When paired with the appropriate feelings, this strategy may be quite powerful. The emotional technique involves using the target's emotions in the conversation to persuade them to do something out of character. Scareware is an example of this from more recent times. A nice illustration would be if a pop-up window alerted users to a system issue that could be resolved by downloading a free update. Their system is only compromised by the upgrade, which is a Trojan horse. alternative emotions that may be exploited in addition to fear include love in all of its manifestations, hate or anger us versus them, pride in oneself or one's organization, and futility there is no alternative course of action. This strategy is built on fear. Selecting the appropriate emotion is simpler in person. After all, we

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

can read body language or over the phone because we can assess voice tone and adapt our approach depending on the circumstance. By manipulating the targets' emotions, this technique hopes to have them overcome their brains' normal cognitive responses [4], [5].

Other popular interrogation strategies include "we know all" and "the file/dossier," when the interrogator enters and places a folder labeled "witness statements" or a DVD labeled "surveillance footage" on the desk. Although they wouldn't include any information, they do enable the interrogator to begin by stating something like, "We have the evidence we need, but we want to get your side of the story before we submit our final report." The presentation of information for SE reinforces the idea that we already know the fundamentals and just need them to supply the specifics. It could be time to attempt the rapid-fire technique, in which we continuously interrupt them until they get irritated and jump in with important details so we will listen. Additionally, it is used when the target is about to say something that the interrogator doesn't want them to say, such as "I never visited that site," since once they speak a lie, it is difficult to persuade them to reveal the truth because we first have to get them to confess, they lied.

False flag operations and "Mutt and Jeff" or "Good cop/Bad cop" are the last two techniques we'll talk about. Everyone has seen the confrontational and sympathetic interview team in films. To protect them from the aggressive one, the target will relate to the caring person and share their tale. A truly nasty interrogator may be followed by one who apologized for the lack of professionalism shown by a colleague. Normally, a good policeman would assist the target in justifying their acts so they could discuss them in public. On social networking sites, for example, SEs may display a Facebook profile made just for the assault as a cyberbully and a second as someone standing up for the victim. The military may have a fresh interrogator enter and appear to be from a friendly nation or a non-governmental organization, such as the Red Cross, as the last application of the false flag. This is helpful since deception is the foundation of social engineering and it is just that.

We can see that the majority of military tactics are immediately transferable to the private sector and may be deployed in both physical and virtual domains. The military's tested tactics, techniques, and procedures (TTPs) and thorough mission planning and preparation are its most crucial contributions. These will provide the assailant a significant capacity to succeed in their goal when used in social engineering.

Military Defends Against Social Engineering

The military has always been involved in the espionage counterspy industry, as was explained in the military approach to SE section. The same abilities required to protect against SE also apply to counterspy tactics. The modern soldier must be knowledgeable in operational security (OPSEC), force protection, counterterrorism, and counterintelligence (CI) procedures. The tactical-level activities that may be taken for CI will be the main topic of this section. Let's first go through the essential ideas' doctrinal meanings [6]:

i. **Counterintelligence:** Information obtained and actions taken to prevent espionage, other intelligence-related operations, sabotage, or murders committed by or on behalf of foreign governments or their agencies, foreign organizations, foreign people, or international terrorist activities.

ii. **Cyber Counterintelligence:** Both foreign intelligence agency collection activities employ conventional techniques to evaluate cyber capabilities and intents and measures to detect, infiltrate, or neutralize foreign operations that use cyber means as their principal tradecraft approach.

iii. **Counterespionage:** This branch of counterintelligence focuses on identifying, penetrating, manipulating, misleading, and suppressing people, groups, or organizations thought to be conducting or suspected of conducting espionage to detect, neutralize, exploit, destroy, or prevent such actions.

iv. **Counterterrorism:** Actions made both directly and indirectly to combat terrorist networks and make the local, national, and international settings hostile to them.

v. **Force Protection:** Efforts made in advance to lessen the likelihood of hostile acts being committed against Department of Defense troops, their families, property, and vital data. Actions to destroy the adversary or safeguard against mishaps, inclement weather, or sickness are not included in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

force protection.

vi. **Operations Security (OPSEC):** A method for locating crucial information and then assessing friendly activity related to military operations and other activities to:
   - **a.** Determine whether behaviors are visible to hostile intelligence systems;
   - **b.** Identify potential signals that opponent intelligence systems may gather that might be analyzed or cobbled together to gain crucial information in time to be valuable to enemies;
   - **c.** Pick and put into effect strategies that make friendly activities less susceptible to enemy exploitation, or remove them altogether.

Military secrecy and confidentiality are essential. They use encryption, data categorization, employee clearances, and a comprehensive set of procedures and rules. Soldiers, Airmen, Seamen, and Marines are aware of the confidence placed in them and the potential amount of national security vulnerability that might result from knowledge loss overall as well as from a single data loss. A crucial part of the National Counterintelligence Strategy now includes cybersecurity. They are increasingly being tasked to protect US economic advantage, trade secrets, and know-how as well as the country from foreign espionage and electronic infiltration of the IC and DoD [7], [8].

As a national concern, counterintelligence is addressed in this US strategy. CI also has an attacking component. To entice insiders to access the information they are not authorized for, traps or as they are known in cyberspace, "honey pots" must be put up. To find out what has slipped out, we need attractive files with built-in beacons that send back location updates. We must support initiatives that provide us access to the kinds of groups with the intent and resources to attack the US so we can discover what they have taken. To determine our degree of preparation, we must do drills and tests on our employees. Finally, we must make sure that those who break the rules face the penalties.

The Army Does CI

Threat Awareness and Reporting Program, Army Regulation (AR) 381-12 The Subversion and Espionage Directed against the US Army or SAEDA Act of 2010 established the counterintelligence training standards and reporting processes on October 4th. Indicators of suspect activity are also included, including links to or influence from outside, contempt for security procedures, strange work behavior, money concerns, travel abroad, excessive curiosity, solicitation of others, and extremist action. In essence, this procedure encourages every employee to take on the role of the security guard and assist in policing both themselves and their colleagues. Situational awareness and behavior monitoring for both themselves and the rest of the team serve as the foundation of the program. If implemented properly, such a program can combat all types of criminal activity, as well as internal risks from unhappy or unstable employees, external threats from foreign operators and terrorists, and modern-day social engineers. When done incorrectly, it may lead to instances like the recent unauthorized leak to WikiLeaks of a significant quantity of sensitive papers pertaining to the US war in Iraq. Although the Navy and Marine Corps are both highly competent in their way at these processes and procedures, we won't go into detail about them here for conciseness.

The "Social Media" Guide has been released by the Air Force Public Affairs Agency. The Air Force and social media Public Affairs Office of the Air Force. Some of the top ten suggestions are: Our objective depends on OPSEC, therefore be mindful of the image you project since it will establish the tone for your communication. If the adversary is engaged, you must join them. This is a great example since it accomplishes a few goals well. The first part of the book focuses more on what we should use than on reasons why we shouldn't utilize the many online communication tools available. Second, it is a written policy with disciplinary repercussions for misconduct [9], [10].

CONCLUSION

The capacity to analyses the material that is being leaked and carry out the necessary investigations to ascertain what steps should be done is a crucial component of this defensive capability. Aldrich Ames, Robert Hanssen, Colonel Vladimir Vetrov, Gregg Bergersen, and the eleven Russian spies recently deported from the US are historical examples, but these operations are time-consuming, expensive, and dangerous when we can obtain much of the same information through cyber spying. The chance of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

being caught is less, access may be gained more quickly, and it costs less money. We've discussed a lot about how to abuse computer networks, and when we combine that with social engineering, our espionage skills change drastically. This necessitates that we examine the methods used to catch these classic spies, including meticulous analysis, financial record auditing, insider information from colleagues, offensive operations to access enemy files to determine who they had converted into spies, and enticing defectors to join our side.

REFERENCES

[1] L. Lugo Urribarri, "Analitica del aprendizaje en un entorno virtual mediante un sistema de computación cognitiva: estudio preliminar," J. Knowl. Manag., 2016.

[2] G. Mediatanto, "Pengaruh Arus Kas Operasi, Arus Kas Bebas, Rasio Leverage, Dan Rasio Profitabilitas Terhadap Kebijakan Dividen," J. Knowl. Manag., 2016.

[3] M. Harb, "Diversifying Urban Studies' Perspectives on the City at War," Int. J. Urban Reg. Res., 2017.

[4] C. Bettin and P. Ordosgoitia, "Estres termico por calor en sector de la construccion: Efectos y consecuencias del calentamiento global," Hum. Relations, 2020.

[5] D. Aryandari, "Hubungan Antara Kesabaran dan Smartphone Addiction Pada Mahasiswa," Hum. Relations, 2020.

[6] I. Apriani, "Upaya Peningkatan Pengetahuan Kader Posyandu Tentang Asi Ekslusif : Literature Review," Hum. Relations, 2020.

[7] Y. Herdianawati, "Strategi Pengembangan Potensi Pariwisata Berbasis Kearifan Lokal Pada Dinas Kebudayaan, Pariwisata, Pemuda Dan Olahraga Kabupaten Ponorogo," Hum. Relations, 2020.

[8] A. E. D. R. PERON, "American Way Of War: O Reordenamento Sociotécnico Dos Conflitos Contemporâneos E O Uso De Drones," J. Knowl. Manag., 2016.

[9] G. H. Arifitama, "Analisis Pengaruh Kualitas Pelayanan Terhadap Kepuasan Konsumen Pada Rumah Makan Mang Engking Di Surakarta," J. Manaj., 2016.

[10] Lembaga Penerbangan dan Antariksa Nasional, "Rencana Strategis Lembaga Penerbangan dan Antariksa Nasional," Lapan, 2020.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of the Surveillance, Data Mining, and Pattern Matching in Cyber Security

Ms. Kasaragod Madhura
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-madhura@presidencyuniversity.in

ABSTRACT: ***Enterprises may evaluate applications more thoroughly than with a single test by using vulnerability assessment and penetration testing (VAPT). An organization may have a more thorough understanding of the vulnerabilities to its applications by using the VAPT technique, which enables the company to better defend its systems and data against hostile assaults. Applications created internally and by outside suppliers both have vulnerabilities, although the majority of these faults are simple to address once they are discovered. While a VAPT provider continues to identify and categories vulnerabilities, using one allows IT security teams to concentrate on mitigating serious vulnerabilities.***

KEYWORDS: ***Cyber Attack, Cyber Security, Vulnerability Assessment, Penetration Testing, Security Management.***

INTRODUCTION

Many big nations now monitor the different forms of communication traveling into and out of their borders, as we described in the Surveillance portion of earlier Chapter of this book. Although this is far from total coverage and flaws in such monitoring may often be identified or made, it does provide some level of protection. Through data mining and pattern matching operations carried out on the communications records we gather, the ability to track communications with those in other countries may be able to give us a warning when coordinated activities, such as attacks, may take place soon, possibly including cyber-attacks [1].

If we look closely at large-scale communications monitoring systems, we may discover many similarities to the well-known Intrusion Detection Systems (IDS) that we often observe running on networks. These systems are essentially IDS running on a much larger scale. These systems may very well act as the technical foundation or forerunners for large-scale IDS that is capable of doing the in-depth analysis of electronic communications that we are used to. We are almost guaranteed to see such capabilities soon, even if the degree of technological complexity required to undertake such actions is absent at the moment and might be classified when created.

One of the main components of a good defense is security policy. We may establish expectations for individuals who create and use the environments that we want to remain secure via the use of rules. Our users' behavior, our software, systems, and networks' setup, among countless other things are all governed by our security policy. In the end, our security guidelines specify precisely what we mean when we term "secure." It is essential to remember that policies issued without the necessary power to execute them are completely meaningless and often disregarded. We need to make sure that the policy is followed in addition to establishing our security via policy, which is done through our compliance activities. The Federal Information Security Management Act (FISMA), the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), the National Industrial Security Program Operating Manual (NISPOM), the Director of Central Intelligence Directive (DCID) 6/3, and numerous other regulations are used in the government to verify compliance. The Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) regulations, and many others are more prominently discussed in the civilian world. Our policies are not worth the paper they are written on or the bits they are stored in if they are not followed. Having said that, it is equally crucial to know that

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

security doesn't cease when compliance is achieved; rather, it serves as a baseline [2].

Intrusion Detection and Prevention

As we described in the last section, it is challenging to identify and prevent intrusions on a national level or even inside the DOD. Currently, most of the networks that make up the Internet are not divided along national borders. In addition, a broad range of media, such as copper and fiber optic cables, satellite communications, purpose-built wireless networks, packet radio, and several more channels, may be used to convey network communications. IDS/IPS deployment is technically difficult due to the absence of network segmentation along physical boundaries and the broad diversity of communication channels.

We can either design networks to provide a small number of connections outside of the area that we wish to protect and monitor, or we can implement massively distributed IDS/IPS, both of which have their own set of problems. The clearest approach is to redesign our networks to have just a few choke points. This approach would be feasible when designing new networks, but it would probably be prohibitively costly for networks that are already in existence. The transition to the cloud and the proliferation of mobile devices will also have an influence. Classified networks are even beginning to consider moving to these new infrastructures as the days of isolated networks are coming to an end. Similarly, although not needing us to change our networks, highly spread IDS/IPS is likely to overlook some of the traffic entering and leaving those networks. In any event, carrying out such activities at the moment is likely to be challenging in several ways.

Vulnerability Assessment and Penetration Testing

Two of the main CND tools are penetration testing and vulnerability assessment. These techniques let us identify the holes in our systems and networks that attackers may use to carry out espionage and surveillance, acquire access, or launch other attacks [3].

Figure 1's mention of vulnerability assessment enables us to, often employ scanning tools like those that identify surface flaws in our systems. Such evaluations often include repeatedly going through our whole system catalog and scanning each one for vulnerabilities using known signatures for those issues. While this may reveal some potential points of entry for attackers, it does not provide a full picture of the potential vulnerabilities in our systems. We need to be considerably more thorough in our efforts and do penetration testing to gain a fuller view of the gaps in our systems.

Figure 1: Illustrated the Vulnerability Assessment.

When done correctly, penetration testing may far more accurately simulate an attacker's attempts to breach our environment. Penetration testing may be carried out from a white box viewpoint, in which case the environment to be attacked is made known to us, or from a black box perspective, in which case we are given no more knowledge than an attacker would typically have. There are several justifications for both strategies, but generally speaking, black box testing is more expensive whereas white box testing more precisely simulates an outside assault. We may also want to think about including extra components in our penetration testing efforts, such as physical security and social engineering.

Making sure that penetration test findings are not hindered to the point where they are useless is one of the risks associated with planning and placing reliance on their outcomes. The aim of adopting the same techniques that possible attackers would use is no longer achieved if we impose limitations on our penetration testing that forbid certain assaults, open-source tools, settings, weapon systems, or even legacy systems. This is true for both practical tests and military drills. These limitations, which are all too typical in penetration testing settings, may both frustrate our efforts and give us a false feeling of security [4].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Disaster Recovery Planning

As a preventative strategy, Disaster Recovery Planning (DRP) may help us endure or recover from assaults, outages, and catastrophes that we were unable to completely avoid. These precautions are often implemented via the use of data backups and various degrees of redundant infrastructure and systems. Although properly maintained backups in the case of CND will undoubtedly enable us to recover in the event of an assault, it is more probable that we will find redundant infrastructure to be more useful in resisting an attack.

Likely, we won't be able to access particular network blocks, domains, systems, etc. in the event of a significant cyberattack. In contrast to the disaster recovery planning that most organizations do, it will probably pay to make sure that our backup sites, from which we may function, are widely dispersed, both geographically and logically. In this manner, we are more likely to have a site that has not been impacted by the assault when we are under attack or need to operate from one. Since this might be difficult for units that are deployed in advance, backup plans like Continuity of Operations (COOP) must be created so the units can carry out their tasks even when the network is impaired or unavailable.

Defense in Depth

Defense in depth is one of the key tenets of an effective defensive strategy. The tiered approach to security is advocated by the defense in depth. In this specific instance, we have network-level, host-level, application-level, and data-level defenses. As an example, we may have access restrictions at the application level, firewalls, and IDS/IPS at the network level, software firewalls and anti-malware technologies at the host level, and encryption at the data level. Additionally, the user awareness training we discussed in the chapter's section on security awareness might be readily included in our tiers of protection. Our crucial information is at the heart of all these levels of protection. Depending on the environment, the layers and security mechanisms at each layer may change, but the fundamental ideas will stay the same [5].

Defense in Depth

Defence in depth is based on the idea that by using several layers of protection, we may either identify our attackers' actions thanks to our components of detection or convince them to stop trying to attack us because our security measures are too strong. This idea is still crucial when we transition to a more mobile device-based network; the difference is that the layers of defense are on the endpoint system rather than the central network.

It may be appealing to believe that we can construct a secure environment and effectively repel any adversary for an endless amount of time, but this is an unreasonable assumption. Instead, we should set up our layered defenses to slow down attackers as much as possible so that we can catch them off guard and respond to their strikes. Additionally, by appropriately segmenting the data on the network and limiting access to each segment following requirements, we can reduce the likelihood that an attacker will be able to enter, steal everything, and then escape.

Different Methods for Cyber Security

The many DM techniques for cyber security are discussed in this section. The following eight are the most widely used large data mining techniques, while there are many more. A brief explanation of each approach is given, along with references to important literature [6].

i. Association Rule

Association rule mining finds the relationship among variables in the database. Let's take an example IF (A and B) THEN C. This rule describes that IF A and B are present, then there is also the presence of C. Association rules have metrics that tell how often a given relationship occurs in the data. Association Rule Mining is a way to discover interesting co-occurrences in supermarket data. It finds frequent sets of items that are combinations of items that are purchased together in at least N transactions in the database, and from the frequent item sets such as {X, Y}, generates association rules of the form: $X \rightarrow Y$ and/or $Y \rightarrow X$.

ii. Clustering

Clustering is used to assign similar data objects in groups called clusters so that the objects in one cluster are more similar to each other than objects in other clusters. In simple words, this process is used to identify data items that have similar characteristics. Clustering is a set of techniques for finding patterns in high-dimensional unlabeled data. The main advantage of clustering for intrusion detection is that it can learn from audit data without requiring the system administrator to provide explicit descriptions of various attack classes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

iii. The Decision Tree Technique

The decision tree is a structure that resembles a tree, with leaves that stand in for classifications and branches that reflect the combination of features that produce those classifications. If-then rules are necessary for decision trees, although metrics and parameters are not necessary. Decision trees may address multi-type attribute issues because of their straightforward and understandable form. Decision trees can also handle noisy data or missing values. They cannot, however, provide the highest level of accuracy that other machine-learning techniques can. Decision trees have the benefit of being easy to implement.

iv. The Neural Network

Neural Networks are inspired by the brain and composed of interconnected artificial neurons capable of certain computations on their inputs. The input data to the first layer activate the neurons of the network whose output is the input to the second layer of neurons in the network. Neural networks are long training times and are therefore more suitable for applications where this is feasible. In the Intrusion detection system, Two kinds of NNs are used [7]:

a) Multilayered feedforward neural networks
b) Kohonen's self-organizing maps.

These techniques are used to model complex relationships between inputs and outputs and to discover new patterns. The combination of a Self-organizing map and back propagation neural network supplies a very efficient means for the detection of new intrusions.

v. Statistical Techniques

Statistical-based systems (SBIDs) take a different approach to intrusion detection. The concept of the SBID system is simple: it determines "normal" network activity and then all traffic that falls outside the scope of normal is flagged as anomalous (not normal). It involves the collection of data relating to the behavior of legitimate users over some time. Then statistical tests are applied to observed behavior to determine a high level of confidence in whether that behavior is not legitimate. It falls into two broad categories:

a) Threshold detection
b) Profile-based anomaly detection

This process of traffic analysis continues as long as the SBID system is active, so, assuming network traffic patterns remain constant, the longer the system is on the network, the more accurate it becomes [8].

DISCUSSION

The paper explored computer network defense (CND) in this part. The defensive and most proactive part of computer network operations (CNO) is called CND. We spoke about how CND falls into the broader category of defensive measures and how non-nation-states could lack the resources necessary to mount a successful defense against a nation-state's all-out assault. We discussed what specifically we want to safeguard in terms of data and information. The CIA trinity of confidentiality, integrity, and availability as well as AAA, which deals with authentication, authorization, and auditing, were some of the other important security concepts that were discussed. These fundamental ideas serve as the cornerstones of the defense of our information assets. We discussed security awareness and training initiatives to safeguard people, who are probably the weakest link in our defenses. We discussed the security attitude and how we may attempt to instill some of it in the users who fall within our purview. After that, we discussed security training for our users so that we could inform them of the appropriate reactions to some of the circumstances in which they can jeopardize our security. We also spoke about how various degrees of technical expertise may need different types of security training [9]–[11].

CONCLUSION

We discussed some of the many techniques that we may use to protect ourselves against an assault while defending against cyber-attacks. We discussed some of the potential applications for the Computer Network Exploit (CNE) surveillance techniques as well as the potential applications for data mining and pattern matching on the obtained data. We also discussed intrusion detection and prevention and how putting these into practice on a very big scale would be challenging. We spoke about how to find the security gaps in our settings using vulnerability assessment and penetration testing as well as some of the ways that these techniques could give us a false feeling of security. Disaster recovery planning was discussed, as well as how we would need to modify it to deal with the reality of cyber warfare. Finally, we took a close look at defense and spoke about how we may integrate multiple layers of protection in our defense. We must always and consistently succeed in computer network

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

defense. Attacks from our adversaries are always possible, and they only need to be successful once. Every assault must be anticipated, and we must respond. This is true for all organizations, networks, and systems. You participate in the continuing conflict as a member of the armed forces, vital infrastructure, or even business systems.

REFERENCES

[1] S. H. Raza, M. Iftikhar, B. Mohamad, N. Pembecioğlu, and M. Altaf, "Precautionary Behavior Toward Dengue Virus Through Public Service Advertisement: Mediation of the Individual's Attention, Information Surveillance, and Elaboration," SAGE Open, 2020, doi: 10.1177/2158244020929301.

[2] B. Haggart, " The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power , S. Zuboff (2018) ," J. Digit. media policy, 2019, doi: 10.1386/jdmp.10.2.229_5.

[3] M. Mulvenna, A. Hutton, V. Coates, S. Martin, S. Todd, R. Bond, and A. Moorhead, "Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia," Neuroethics, 2017, doi: 10.1007/s12152-017-9305-z.

[4] A. E. Clarke, L. Mamo, J. R. Fishman, J. K. Shim, and J. R. Fosket, "Biomedicalization: Technoscientific transformations of health, illness, and U.S. biomedicine," Am. Sociol. Rev., 2003, doi: 10.2307/1519765.

[5] W. Lestari, "Pengaruh Pelayanan Promosi dab Syariah Terhadap Minat Nasabah Dalam Memilih Asuransi Syariah (Studi pada PT.Asuransi Takaful Keluarga Cabang Palembang)," J. Chem. Inf. Model., 2019.

[6] J. D. Jensen, "Knowledge Acquisition Following Exposure to Cancer News Articles: A Test of the Cognitive Mediation Model," J. Commun., 2011, doi: 10.1111/j.1460-2466.2011.01549.x.

[7] A. Comin, J. Grewar, G. van Schaik, H. Schwermer, J. Paré, F. El Allaki, J. A. Drewe, A. C. Lopes Antunes, L. Estberg, M. Horan, F. F. Calvo-Artavia, A. H. Jibril, M. Martínez-Avilés, Y. Van der Stede, S. E. Antoniou, and A. Lindberg, "Development of Reporting Guidelines for Animal Health Surveillance—AHSURED," Front. Vet. Sci., 2019, doi: 10.3389/fvets.2019.00426.

[8] B. Omar, "Immediacy Gratification in Online News Consumption and its Relations to Surveillance, Orientation and Elaboration of News," Procedia - Soc. Behav. Sci., 2014, doi: 10.1016/j.sbspro.2014.10.313.

[9] J. D. S. Silva, J. C. M. Calçada, S. O. Rezende, and D. B. Calçada, "Automatic identification of knowledge related to dengue cases in the state of piauí in public databases using filtered-association rules networks," Rev. Inform. Teor. e Apl., 2020, doi: 10.22456/2175-2745.99849.

[10] F. Gil-Olivares, H. Manrique, L. Castillo-Bravo, L. Perez, G. Campomanes, K. Aliaga, J. Lagos, A. Aguilar, and G. Umpierrez, "Management of glycemic crises in adult patients with diabetes mellitus: Evidence-based Clinical Practice Guideline, Lima - Peru.," Rev. la Fac. Med. Humana, 2021, doi: 10.25176/rfmh.v21i1.3194.

[11] D. Pardoll, "Does the immune system see tumors as foreign or self?," Annual Review of Immunology. 2003. doi: 10.1146/annurev.immunol.21.120601.141135.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Analysis of Challenges in Cyber Security

Mr. Sudhakar Deepak Raj
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-deepakr@presidencyuniversity.in

ABSTRACT: ***Today, the key element of the nation's entire national security and economic security strategy is cybersecurity. There are a lot of cybersecurity-related issues in India. Every organization requires a security analyst to ensure that their system is safe given the rise in cyber-attacks. These security analysts must secure private organization servers, protect the secret data of governmental organizations, and other cybersecurity-related difficulties. technical difficulty. Every IT system has an "attack surface" that an intruder may take advantage of. This attack surface is still being expanded by API-based design and cloud-based technologies. Legacy systems are also much too thick and complicated to be readily protected against hackers.***

KEYWORDS: ***Cyber Attack, Cyber Security, Hacking, Internet Security, Network Security.***

INTRODUCTION

Based on research completed for a white paper created by TASC as part of the CTO's office Cybersurfed program, this chapter. To decide where resources should be allocated most effectively, the research was created to assist consumers in understanding the full range of cyber issues they now face. The University of Virginia Applied Research Institute collaborated on it. Steve Winterfeld, Anthony Gadient, Kent Schlussel, and Alfred Weaver were the original writers. It is being used here with their consent [1].

Right now, the United States (US), Western Europe, and a large portion of Asia have completely integrated the Internet into their economies and militaries to the point where they rely on it for day-to-day operations. These digital skills have developed into a key hub for the US. The majority of other countries are also heading swiftly in this direction. There are an increasing number of stand-alone, networked, and web-based systems (computers, mobile devices, infrastructure devices) and apps that offer this cyber capability. Nations deal with systems that are rife with flaws that might easily affect our capacity to uphold secrecy, verify integrity, and guarantee availability as a result of this tremendous expansion. National cybersecurity concerns have been significantly exacerbated by this growing dependence on technology. In Figure 1 below, current significant cybersecurity concerns are shown:

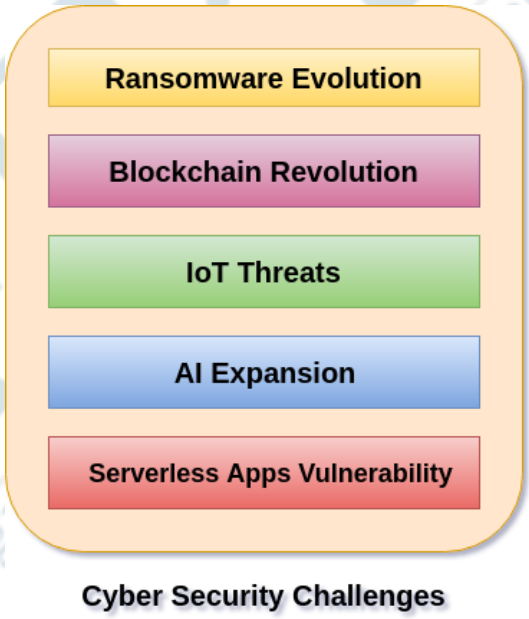

Figure 1: Illustrated the Different Cyber Security Challenges

Ransomware Evolution

A kind of virus known as ransomware encrypts data on a victim's computer and demands money to release it. The victim regained access credentials after a successful payment. The scourge of IT, executives, data specialists, and cybersecurity experts is ransomware. In the realm of cybercrime, ransomware assaults are on the rise. To safeguard their firm, IT

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

experts and business executives must have a strong recovery plan against malware assaults. The recovery of business and customer data and applications must be properly planned for, and any breaches must be reported under the Notifiable Data Breaches system. The greatest defense against ransomware assaults nowadays is provided by DRaaS solutions. When malicious assaults compromise our data, we can simply determine which backup is clean and initiate a fail-over with the push of a button thanks to DRaaS solutions [2].

Blockchain Revolution

The most significant development of the modern computer age is blockchain technology. We now have a native digital medium for peer-to-peer value exchange for the first time in human history. A technology that makes cryptocurrencies like Bitcoin possible is the blockchain. A transaction or business may be conducted between two or more parties using the blockchain without the requirement for a third party to build trust. What blockchain systems will bring in terms of cybersecurity is impossible to foresee. Cybersecurity experts can hazard some informed assumptions about blockchain. There will be a healthy tension as the use and value of blockchain in the context of cybersecurity develops, as well as complementing integrations with conventional, tested cybersecurity measures.

IoT Threats

The Internet of Things is referred to as IoT. It consists of a network of connected physical objects that may be accessed online. The linked physical devices may transport data over a network without requiring any human-to-human or human-to-computer contact and have a unique identification (UID). IoT device firmware and software render consumers and organizations very vulnerable to cyberattacks.

IoT devices weren't developed with cybersecurity and commercial uses in mind when they were created. To manage risk, every organization must collaborate with cybersecurity experts to guarantee the security of its password rules, session management, user verification, multifactor authentication, and security procedures [3].

AI Expansion

Artificial intelligence is referred to as AI in short. The science and engineering of creating intelligent devices, particularly clever computer programs, is what John McCarthy, the founder of artificial intelligence, characterized as AI. The development of intelligent machines that function and behave like people is a field in computer science. Speech recognition, learning, planning, problem-solving, and other tasks are some of the activities associated with artificial intelligence. The main advantages of incorporating AI into our cybersecurity approach are its capacity to defend and safeguard an environment when a harmful assault starts, hence reducing the damage. When a danger affects a firm, AI takes fast action against harmful assaults. AI is seen as a potential defensive measure that will enable our company to remain ahead of the cybersecurity technology curve by IT business executives and cybersecurity strategy teams.

Serverless Apps Vulnerability

Applications using serverless architecture or back-end services, such as Google Cloud Function, Amazon Web Services Lambda, etc., rely on external cloud infrastructure or back-end services. Because users use the applications locally or off-server on their devices, serverless apps encourage hackers to distribute malware on their systems with ease. As a result, while utilizing serverless applications, the user should take security safeguards.

As a result, US adversaries of all stripes, such as hackers (anyone engaging in unauthorized activities on a system), insider threats, hacktivists (hackers motivated by a cause), industrial spies, organized crime, terrorists, and national governments (often referred to as Advanced Persistent Threat or APT) now possess a fundamental but operationally significant technical capability. "It's now obvious that this cyber threat is one of the most significant economic and national security challenges we face as a nation," stated President Barack Obama. Additionally, neither the government nor the nation is as prepared [4].

The authors have added to their initial list of core difficulties as a result of the TASC team's review of various papers while researching this topic. There is no single document that concisely and thoroughly identifies the cyber challenges facing the US and Department of Defense (DoD) and organizes these issues so that senior leaders can develop an all-encompassing plan to address the issues facing their organizations and technical staff can determine which challenges most directly affect their organization. This chapter fills the gap in three different ways. First, it offers a succinct summary and taxonomy of the main

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

cyber threats the US and DOD are now experiencing. It then outlines who should give resources to the various problems. Finally, it offers a glimpse of what is ahead. It is not intended to provide solutions, but rather to spark conversation about the next measures that should be taken to position the US for success in the internet.

Cybersecurity Issues Defined

These issues were examined from a national perspective and might need modification for particular units or organizations. The problems were chosen after considering input from customers, the TASC Cyber Community of Excellence, and studies like the Institute for Information Infrastructure Protections' (I3P) National Cybersecurity R&D Challenges, the Networking and Information Technology Research and Development's (NITRD) National Cyber Leap Year, InfoSec's Hard Problem List, the Computing Research Association's Four Grand Challenges in Trustworthy Computing, and the Department of Energy's A scientific R&D challenge Based on the greatest problems they believe our country is experiencing, the writers chose the final list. They recognize that certain topics may be argued to be included, while others that are already there might not be important to specific organizations or would be better categorized [5].

The difficulty of each issue has been categorized by the writers. Extremely difficult (ED), very difficult (VD), difficult (D), and not cost-effective (NCE) are the order of difficulty. We have attempted to measure and categories the complexity and kinds of resources required since there is no clear method to rank them because the resources needed for each task vary. It takes traditional research and development to create new technologies in some circumstances, political will in others, regulations in others, and money in all cases at some level. We have also divided the difficulties into groups according to the resources needed, with each group being designated as follows: Very Important = $$$, Significant = $$, and Less Important = $. We will use the initial unclassified CNCI budget of 9 billion as very significant, less than 4 billion as significant, and less than 1 billion as less significant, even though it is challenging to address how to categories levels of resources because different challenges required different methods to solve in general. These are extremely rough estimations, and the number of resources needed would need to be determined by comparing each issue to a particular strategy. [6].

To highlight the links among the problems, they are categorized. The three main categories are people, policy, and technical. The areas of overlap between them are that people and policy share organizations, technical and people share skills, and policy and technical share processes. The mapping in Figure 2 illustrates the core set that is shared by all challenges. As each organization would rank these concerns differently depending on their dangers, they are not presented in any particular priority order.

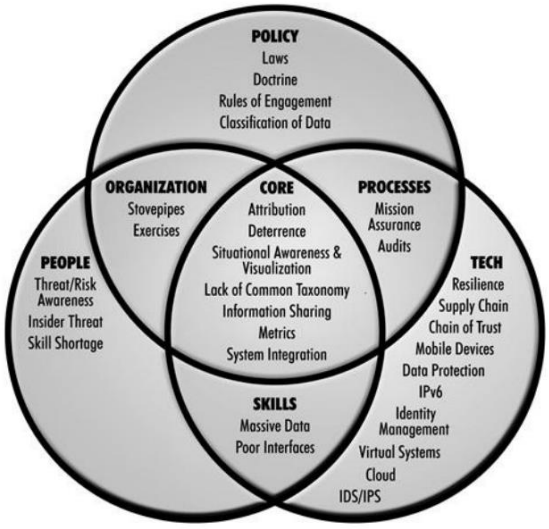

Figure 2: Illustrated the Categorization and Relationships of the Challenges.

Policy

Laws (ED $) cover matters of policy, law, privacy, and national security. These concerns often clash with one another in the US today. Our laws are influenced by our background and culture. Cyber concerns are relatively young compared to the history of our legal system, which dates back to common English law and the Magna Carta in 1215. In establishing limits for many of today's technology advancements, such as those in cyber, medical, and communications, our legal system lacks expertise. The legal concerns are further complicated in the US since each state enacts its laws that range greatly from one another, and even federal law is subject to diverse interpretations by different courts.

The doctrine (VD $) that addresses offensive and defensive cyber strategy via tactics, methods, and procedures suffers from a lack of uniformity throughout the armed services. This is not to imply that there is no doctrine at all or that it is in conflict,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

but rather that there is no one, shared doctrine. The DOD has advanced by creating a consistent vocabulary. Additionally, each service has established commands, and CYBERCOM has been established at the Joint level. The issue that there is no shared understanding of cyber operations and cyberspace warfighting doctrine persists [7].

Rules of Engagement (ROE) (VD $) are necessary for local commanders who understand how to respond to kinetic or real-world attacks based on approved ROEs, but in cyberspace, there is no consensus on what constitutes an "act of war" or "use of force" on the Internet, so there is no established doctrine on how to fight a cyber-war. In the event of an attack, the attribution of the attacker will not always be successful. What defines an incident or attack and the appropriate course of action (technical, legal, or diplomatic) must be clearly defined.

There are problems with data classification (D $$) since various practices are used for data categorization by different US federal organizations, which makes it difficult to collaborate with non-DoD organizations. Although there is a single formal set of guidelines, the several agencies that deal with classified material apply them quite differently. The exchange of data across agencies may often be challenging when you consider that each organization has a distinct culture. People may not be able to fully interact and discuss specific issues outside of the Intelligence Community (IC), the rest of the DOD, and other non-IC entities owing to a lack of clearance. There is a movement to raise the number of individuals with clearances, but it won't solve the problem since each crisis will call for a different group of specialists to solve it, and it's impossible to know who will be required in advance. We want a solution that can exchange data while maintaining operational security, depending on necessity rather than background checks.

Processes

The objective of mission assurance (ED $$) is on safeguarding networks and data while conducting operations. To ensure that the operational duties are completed in order to fulfil the organization's objective, it is necessary to engage in combat via a disputed cyber domain this includes military systems, the Defend Industrial Base, and the commercial backbone networks they employ. What is required is knowledge of which systems are essential for carrying out the mission and how they can be used in a degraded mode i.e. using a constrained or alternative set of protocols to maintain maneuverability and fundamental capabilities in a situation where they may no longer have control [8].

Audits (D $) are the regular, structured evaluation of an enterprise's cyber systems, personnel, and processes. The audit process represents the measurement step in a continuous cybersecurity improvement program (implement → measure → correct). As such, regular cyber audits represent the keystone of any cybersecurity program. However, in a recent cyber audit of the Department of Homeland Security (DHS) performed by the Inspector General (IG); the DHS IG noted that, "Adequate security controls have not been implemented to protect the data processed from unauthorized access, use, disclosure, disruption, modification, or destruction".

We may question why a cyber-audit of the organization charged with the protection of the US homeland would uncover over 600 vulnerabilities, including 202 rated as high-risk, given the significance of the cyber audit as a component of any cybersecurity program. It's easy to see why. A collection of clearly specified rules cannot currently be easily checked against accounts, data, employee behavior, and security setups. We need to create a set of standards that the government and business can utilize as a foundation for creating an automated cyber auditing capacity in order to prevent outcomes similar to those seen by the DHS IG.

We have the present set of Certification and Accreditation standards that are used today, which is a significantly different direction. The Director of Central Intelligence Directive (DCID) 6/3 process, the Federal Information System Management Act (FISMA) process for all government agencies, and the DOD Information Assurance Certification and Accreditation Process (DIACAP) are all being modified to be more focused on real-time monitoring. An excellent illustration of where they are going is the NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations (Draught Dec 2010).

Technical

Systems are intended to self-heal via resilience (ED $$$) without the need for human intervention. In the context of cyberspace, a robust cyber system must function (as intended) even if it is compromised, as may happen if unauthorized access is gained. It should be emphasized that this is not the same as

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

reconstitution, disaster recovery planning, or continuation of operations planning (COOP). Given the extremely dispersed nature of modern cyber systems, resilience refers to a system's capacity to perform its intended function in the face of denial-of-service assaults that might jeopardize network access. Therefore, resilience is a quality we require in our cyber systems. As a result, creating a resilient system and, in particular, designing an enterprise-level system to be robust in a disputed cyber warfare environment, is a problem [9].

Supply Chain (ED $$$) refers to the design and production of hardware and software, both of which are increasingly carried out abroad. Software and hardware with no external components are very rare. Hardware verification and validation have become much more challenging as hardware complexity has increased. We can confirm that hardware performs as promised if we can authenticate all of the interactions between system hardware components.

The difficulty is in how hardware and software authentication is carried out. Software or firmware loads are often included at various phases of manufacturing, and many hardware components originate from several (and sometimes rival) suppliers. To ensure that the device performs as promised and that there are no hidden capabilities that could harm the entire system, create covert channels, or create unknown vulnerabilities that could be exploited by advisories (whether they be nation states or criminals), every interface and transaction must be authenticated. A prospective enemy deliberately including a logic bomb in a hardware implementation is one example of the difficulties that result from a supply chain. Given the considerable amount of integrated circuits that are produced in Taiwan and China, this is especially concerning [10], [11].

DISCUSSION

If we can verify all interactions among corporate hardware serving the computing demands of enterprise users, we can increase the level of trustworthy computing in an enterprise context, which is where the chain of trust (VD $$) originates from. An attack utilizing a man-in-the-middle technique is prevented or made much more difficult by using hardware that can authenticate each connection. An example would be if a command-and-control system sent an order to a weapon's system: how would the sender know it was received, how would the receiver know it was really from the command-and-control system, and how would both parties know the message's contents hadn't been changed? As more mobile devices (VD $$) like as cellphones, thumb drives, iPads, and laptops connect to the grid, it is necessary to both safeguard them and verify their security before connecting. These devices are often linked to secure networks where they are used to perform critical business with little to no security oversight. It is getting more difficult for the security staff to stay up to speed with events as the younger generation of employees brings technology from home to the workplace and uses personal devices for work.

CONCLUSION

IPv6 (D $$) is a problem since switching to the new protocol will open up new chances for both attackers and defenders. The IPv4 Internet Protocol (IPv4) addresses assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) are expected to run out in 2012. Over the next several years, IPv6 installation will be compelled as a result. Finding people with IPv6 expertise and updating equipment will be the biggest challenges. As a result of the new protocol's many addresses, it will be resource-prohibitive for an organization to scan every network address, which will need a change in strategies and equipment. Despite being less developed, the protocol has more security features, thus if it is widely used, it should provide greater security. Instead of defending the network or operating system, data protection (D $) focuses on ensuring the data's confidentiality, integrity, and availability. Today, many businesses concentrate their cybersecurity efforts on fortifying the digital perimeter with tools like firewalls. This "line in the sand" or "Maginot Line" approach ignores the fact that the data stored on an organization's cyber systems account for a significant amount of the value of its cyber assets. Along with papers, this information also contains emails, online pages, web applications, and important executables like operating systems. Classifying their data by level, significance, or worth is a challenge that many organizations would need to overcome initially. Therefore, in addition to any perimeter defence operations, a complete cyber plan should give data security a high priority. This information-centric perspective raises important issues. We must consider if a perimeter defense is the best strategy for data security or whether an asymmetric, decentralized defense is necessary. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

remedy is to switch to a different model since the answer is no.

REFERENCES

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," Comput. Secur., 2017, doi: 10.1016/j.cose.2017.04.005.

[2] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocess. Microsyst., 2020, doi: 10.1016/j.micpro.2020.103201.

[3] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges," Int. J. Inf. Secur., 2021, doi: 10.1007/s10207-020-00503-w.

[4] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," Future Internet. 2019. doi: 10.3390/fi11030073.

[5] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Computers and Security. 2016. doi: 10.1016/j.cose.2015.09.009.

[6] A. Mihailović, J. C. Smolović, I. Radević, N. Rašović, and N. Martinović, "Covid-19 and beyond: Employee perceptions of the efficiency of teleworking and its cybersecurity implications," Sustain., 2021, doi: 10.3390/su13126750.

[7] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: a review and research agenda," Supply Chain Management. 2020. doi: 10.1108/SCM-10-2018-0357.

[8] R. Zuech, T. M. Khoshgoftaar, and R. Wald, "Intrusion detection and Big Heterogeneous Data: a Survey," J. Big Data, 2015, doi: 10.1186/s40537-015-0013-4.

[9] N. Etemadi, Y. Borbon-Galvez, F. Strozzi, and T. Etemadi, "Supply chain disruption risk management with blockchain: A dynamic literature review," Information (Switzerland). 2021. doi: 10.3390/info12020070.

[10] A. Saravanan and S. S. Bama, "A Review on Cyber Security and the Fifth Generation Cyberattacks," Orient. J. Comput. Sci. Technol., 2019, doi: 10.13005/ojcst12.02.04.

[11] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability challenges in the cybersecurity information sharing ecosystem," Computers, 2020, doi: 10.3390/computers9010018.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of Identity Access Management in Cyber Security

Mr. Himanshu Garg
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-himanshu@presidencyuniversity.in

ABSTRACT: ***Identity Access and Management is abbreviated as IAM. In simple words, it restricts access to sensitive data while allowing employees to view, copy and change content related to their jobs. This information can range from sensitive information to company-specific information.It refers to the IAM IT security discipline as well as the framework for managing digital identities. It also deprives the provision of identity, which allows access to resources and performing particular activities. When you exceed your target, IAM ensures that the appropriate resources, such as the database, application, and network, are accessible. Everything is proceeding according to plan.***

KEYWORDS: Cyber Security, Confidentiality, Cyber Attack, Identity Access Management, Vulnerability.

INTRODUCTION

Identity Management (IDM) (NCE $$) consists of three functions that need to be accomplished when allowing personnel to access the network: authenticate them are who they say they are, authorize what they have access to, and audit what they do. The days of IDM being just an 8–12-character password are dead. Today most companies are moving to tokens or biometrics to help ensure they are authenticating the individual. They are also building rules that limit what each individual can do so they only have access to what they need to do their jobs. The issue is that there is no common standard today. There are efforts like the DHS which has published a draft of the National Strategy for Trusted Identities in Cyberspace which could help at the national level. Virtual Systems (NCE $)/Cloud (NCE $) may occur at many levels for example hardware, memory, storage, software, data, desktop, network, or entire data centers. Virtualization at the level of the operating system (OS) permits the hosting of multiple virtualized environments within a single OS instance. Applications can be virtualized, allowing them to be hosted independently of the underlying OS. Cross-platform virtualization allows software written for a specific central processing unit (CPU) and OS to nevertheless operate on different CPUs and OSs. At the top level of abstraction, a Virtual Machine (VM) is a software implementation of an operating system or computer. At the network level, virtualization allows access to applications, data, and computing resources through the Internet which is also known as cloud computing [1].

For reasons of security and governance, clouds can be deployed as public, private, or hybrid. Public clouds are those data centers outside a user's firewall and are provided by third parties. Private clouds remain within a user's firewall; hybrid clouds offer a mixture of both. From a security point of view, virtualization has issues with configuration management, patching, cross-platform attacks, and auditing. Cloud computing has issues with shifting applications, data management, and processes to a third party set of configuration standards, control/ownership over sensitive data, reliability of the company hosting the data, applicable laws, and lack of physical control. Security and confidentiality are crucial issues for a successful transition to these technologies. In addition, there are legitimate concerns over performance variability, reliability, and resilience of cloud-based services.

Intrusion Detection Systems (IDS)/Intrusion Protection Systems (IPS) (NCE $$) monitor the network to detect signatures of known malware or patterns of activity that are unauthorized. Today, significant attention is paid to protecting our IT systems to prevent intrusion. The philosophy underlying this is that if only authorized individuals have access to the cyber systems, those systems are to a large degree protected. The philosophy driving interest in intrusion detection is that if no intrusion is detected, then it can be inferred that only authorized individuals are accessing the system and the system is de-facto safe, per our earlier discussions, insider threat does not go away. However, ignoring the challenges

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

represented by Insider Threats, Intrusion Detection is in itself a challenging problem. Today most security detection systems are signature-based, yet signature-based defenses are inherently perimeter-focused, and state-of-the-art cyber threats tunnel through or go around these defenses. Also, Intrusion Detection systems only show what they catch, not what they are not catching, so if there is no signature in place, the attack may go completely unnoticed. Looking forward we must detect and protect against zero-day exploits [2].

Skills

Massive Data (VD $$) is the result of so much data being collected that there needs to be a way to stop data mining and start real-time correlation. Today logging is a challenge; the classic debate is how much needs to be done because it raises costs. Most large networks (over 10,000 users) don't have the resources to log more than a few weeks' worth of data and even that is not truly analyzed. We need systems and processes that allow us to do long-term trend analysis (over a month not just days or weeks).

Poor Interfaces (D $) are problematic as most systems are not designed to allow a user to rapidly manipulate information at the rate it is coming into the database. Those who have ever been in a Security Operations Center know it is not unusual to see Intrusion Detection System (IDS) events scrolling off the screen. We need security systems that are intuitive and allow the analysis to develop and manage the investigations in a way that provides an advantage rather than just a person reacting to what they are provided.

People

Threat/Risk Awareness (ED $$) is a concern because most users today implicitly trust their computer system when they log on, they assume emails are sent from the displayed sender and they don't think attachments like Word documents could contain malware. This behavior issue must be addressed. We need to change the mindset of the user to "trust but verify" when they log on. Users should understand how to validate their security and know what kind of indicators to look for in a compromised system. We don't expect everyone to become a cyber-security expert but we do want them to have basic survival skills to keep their information secure. One simple example is to use encrypted email when discussing sensitive material. There needs to be a national program, for the awareness it could be based on the "Smokey the bear says stop forest fires" or "This is your brain on drugs" campaigns [3].

Insider Threat (NCE $$) is quite possibly the greatest challenge. The definition of who is an insider has been debated. Most people automatically think an insider is an employee, a student, or other member of the staff of a host institution that physically operates a computer system. These people have a legitimate reason to access the cyber systems and can be considered insiders. However, it can be many other types of people:

- **i.** A contractor, associate, business partner, etc…., someone who has a business relationship with the institution that hosts the computer system.
- **ii.** An authorized person that is allowed to perform limited operations (e.g. a bank's customer who uses the bank's system to access his/her account or a student who is allowed to access grades).
- **iii.** A person who has been coerced or duped into performing certain operations on an outsider's behalf.
- **iv.** A former insider possessing access credentials that were not revoked when terminated.
- **v.** A former insider who created "secret" credentials to give his/her access at a later date.

There are many reasons why a person behaves maliciously. Some of these are for ideological reasons: revenge, the ego that proves the insider can just do it, and plain greed. While people have not significantly changed in the last 20 years, the technical and economic landscape of the US has changed significantly. Technology advances and e-commerce has made it easier for the insider to gain access to critical information. This problem will continue to get more complex as the world becomes more interconnected. We need to increase our ability to use role-based management and real-time auditing [4].

Skill Shortage (NCE $$$) is influenced by the general lack of skilled cybersecurity engineers today and the poor pipeline for new talent coming out of the schools. In the report Human Capital Crisis in Cybersecurity Jim Glosler NSA visiting scientist and founding director of the CIA's Clandestine Information Technology Office was quoted saying there are only about 1000 security specialists in the US who have the specialized skills to operate effectively in cyberspace:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

however, the US needs about 10,000-30,000 such individuals. There is a severe shortage of skilled cybersecurity professionals to address the needs of the force today, as many of the US's top cybersecurity minds are "unclear able" or have no interest in working for the government or the military. Also, educational programs focusing on cybersecurity at institutions of higher learning are still in their infancy. In March of 2010 the administration did kick off the National Initiative for Cybersecurity Education (NICE) and DHS/NSA has the Centers for Academic Excellence in Information Assurance Education but there is no national-level effort [5].

Organization

Stovepipes (D $) are built around Computer Network Operations (CNO) functions and while it may be easy to separate different "disciplines" of cybersecurity for discussion points, they are all interrelated to one another in practice. When we look at Computer Network Operations, which consist of Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE), we see them treated as separate disciplines and there is little to no crosstalk or collaboration. All three disciplines need to integrate the offense (CNA) with the defense (CND) and enable them with intelligence (CNE). The DOD does this today in the kinetic world and needs to apply the same processes to the virtual battle space across the different organizations that control these capabilities. There are also stovepipes built along budget or organizational structures but this issue is aimed at integration of CNO.

Exercises (D $$) challenges are based on a need to practice responses to every situation. This is increasingly the case when applied to organizations. When we look at the number and types of exercises today there is simply a lack of both focused and integrated exercises to understand the responses to a cyber-event. Generally, the rules that limit current cyber exercises do not accurately reflect the level of impact cyber is expected to play in a real-world conflict so organizations are not training as they expect to fight. So if cyber is considered to be another domain of warfare (others being land, sea, air, and space), there has been no unifying doctrine to understand the various aspects of "cyberspace" or Tactics Techniques, and Procedures (TTPs) that would come out of exercises. Note that there are some efforts like Cyber Shockwave and Cyber Storm but cyber needs to become a ubiquitous aspect of exercises.

Core (Impacting All Areas)

Attribution (ED $$$) for cyber is the process of determining who conducted an activity. There are three types of attribution in cyberspace: geolocation (facilitates kinetic military type strike), tracking a cyber-identity (facilitates the intelligence community tracking activity of a specific person or group), or tying a person to the keyboard (facilitates a criminal investigation). It is worth noting many technical attribution capabilities are not allowed due to policy or legal restrictions [6].

The ability to identify, beyond a reasonable doubt, the originator of a cyber-attack is essential to enable an effective and legal response. Given the virtual nature of the cyber challenge, the collection of forensic evidence takes on a new life what is the cyber equivalent of a fingerprint or DNA? What does the "reasonable doubt" threshold mean in a virtual world? To complicate things further, if investigators can trace an attack, what can be done with the results? For the military what level of intelligence is sufficient to authorize an attack? Fundamentally, today there exists no way to reliably identify the original attacker.

In his testimony before Congress, General Alexander stated that: "Conflict in cyberspace, moreover, is highly asymmetric. Minor actors can afford and deploy tools to magnify their effects; witness the recent press reports about arrests in Europe of several individuals charged with creating the so-called "Mariposa botnet" a collection of 13 million computers slaved together for criminal purposes. The tools these actors can employ are almost anonymous a defender can sometimes learn where an attack came from, but can be time-consuming. That means "attribution" in cyberspace is costly and comparatively rare. The "price" an adversary pays for a capability a tool or weapon can be slight; the cost and impact borne by the victim of the attack can be very high"[7].

Deterrence (ED $) is associated with what will happen if we launch a cyber-attack or practice poor cyber behavior. Deterrence only occurs when there is something a legal rule, cultural taboo, or consequence that makes us not "attack" a system, knowing full well what happens when we get "caught." The most critical aspect of Deterrence is to make the cost/benefit ratio change from today's high benefits and low cost or risk to us where the costs outweigh the benefits. This can be accomplished by making the cost of the attack very high by either increasing the barriers so that an effective attack requires significantly more resources

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

to perpetrate, or by increasing the cost of retaliation by improving the chance of detection. Situational Awareness & Visualization (ED $$) is the correlation and fusion of data from multiple sources that enables decision-making. This is, at best, poorly understood today. Situational awareness allows leaders to make informed decisions. There are many Common Operational Pictures (COP) and dashboards today, but they fail to facilitate true risk posture understanding and/or provide information in a format that enables decisions. If the data does not facilitate a decision, it will soon be ignored. The types of data and their presentation should be driven by the types of decisions that must be made. It will vary at different levels of an organization and for different functions within any organizational level but today they are driven by the type of data available. First, the roles need to be set, we must understand what decisions need to be supported and finally, the standards for implementing how we present information to the different audiences need to be established.

Lack of common Taxonomy (VD $) issues revolve around the need for a standard "language" for cyber topics. When we read or discuss computer security, network security, InfoSec, Information Assurance, cybersecurity, or cyber war, we must be careful to understand the terms that are being used and that everyone is using the same definition. There is no industry standard, government regulation, or international agreement on what is meant by simple terminology like "intrusion". This can quickly lead to confusion when trying to have a diverse group of professionals analyze an incident. Within DOD there was so much confusion on what malware was called they hired MITRE to establish a Common Vulnerabilities and Exposures (CVE) database. There needs to be an international body that determines the definitions for IT terms that will be used by the technical community, governments, and legal authorities.

Information Sharing (D $$) is a challenge in the sense that people like to share most information except for what they believe to be private. However, this is not the case for governments and corporations. Corporations often do not share information simply due to competition, and governments do not share information for matters of national security. In the cyber world, the question arises whether corporations and governments should share information on cyber-attacks [8].

However, there are cases where we may want to keep cybersecurity issues limited to a few key personnel. Some examples of these cases are: don't want to expose a vulnerability, desire to protect reputation, need to limit liability or cost of participation in the external investigation. Efforts in one area often do not share information with efforts in another despite being interrelated. Knowledge transfer in a large organization is more difficult due to the size and communications flow. There are also several public/private efforts that the government is trying to get industry to share information but these efforts are not coordinated and many of them are only achieving limited success [9].

Metrics (D $) revolve around the need to quantify the impact of malicious and suspicious cyber activity. Just as there is no common understanding of definitions for cyber topics, there also exists no set of predefined, industry-standard metrics for cyber activities. Metrics for cyber are difficult to implement because of varying definitions of what is needed and important. For example, how we measure Return on Investment (ROI) is varied based on what organizations see as important. There are three basic types of metrics:

i. Technical: Most organizations track how many intrusion attempts were stopped, how many viruses were detected, the number of days/hours systems were up, communications exchanged (email, IM), a number of incidents closed out.
ii. Security: If an organization introduced new processes to detect intrusions that increased detection by 20% or lowered cost by $50,000, or introduced a new tool in the Security Operations Center that cut time to accredit systems by 17 weeks. These goals must be set before the change and methods to track performance are established.
iii. Risk Posture: Example's include: when an organization is connected to new partner networks and it impacted our risk by 40% or our external router was compromised and it lowered our security posture to yellow because it forced us to change the access control list to block IP ranges that were attacking us without normal configuration control processes.

DISCUSSION

Many groups are working on this issue including the Administration's CIO's IT Dashboard and the IT Workforce Committee's Importance of Effective

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Performance Metrics studies, but these are not getting the level of wide acceptance needed. The solution may be regulatory, legislative, or industry best practices, but there needs to be a standard so we can measure the impact and benefits of our actions. System Integration (D $$) is the desire to overcome the common practice today of an organization purchasing multiple point security systems that do not work together and instead, get one system that coordinates and correlates protection activities. Most security systems used today have a specific function. For example, an organization may have a firewall, an intrusion detection system, anti-virus and anti-spyware tools, forensics tools to help with attribution, network management and monitoring systems including packet sniffers, encryption/decryption capabilities, virtual private networks, patch management systems, web activity filtering, password, and log activity correlation. Each of these systems produces logs that need to be correlated together to provide a view of the overall system health and risk posture. This type of correlation is only possible through the appropriate integration of our subsystems and is essential to address a variety of cyber threats including the ability to identify and track potential insider threats. However, too often today's subsystems act as a series of point tools that do not interact to achieve the synergistic effects integration can provide [10].

CONCLUSION

It should be noted that, while systems integration can provide numerous benefits, including enabling a completer and more integrated operational picture of the cyber threat, it also increases the risk that, like dominos, an effective cyber-attack that brings down one subsystem causes the entire system to fail. This highlights the importance and needs for resilience and represents an important challenge in architecting the cyber enterprise. Just as in insurgency warfare, there is a trade-off between pushing down control to the lowest levels to allow small units to act independently versus having more centralized control to enable larger coordinated efforts. Likewise, the architecting of a robust cyber enterprise faces similar challenges. We cannot continue to have multiple-point solutions; we need a unified framework.

REFERENCES

[1] M. Abu-Alhaija, "Cyber security: Between challenges and prospects," ICIC Express Lett. Part B Appl., 2020, doi: 10.24507/icicelb.11.11.1019.

[2] S. V. Sudarsan, O. Schelen, and U. Bodin, "Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3093327.

[3] R. Bruzgiene and K. Jurgilas, "Securing remote access to information systems of critical infrastructure using two-factor authentication," Electron., 2021, doi: 10.3390/electronics10151819.

[4] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," Glob. J. Health Sci., 2016, doi: 10.5539/gjhs.v9n3p157.

[5] C. L. Hsu, W. X. Chen, and T. V. Le, "An autonomous log storage management protocol with blockchain mechanism and access control for the internet of things," Sensors (Switzerland), 2020, doi: 10.3390/s20226471.

[6] S. Devlekar and V. Ramteke, "Identity and Access Management: High-level Conceptual Framework," Rev. Gestão Inovação e Tecnol., 2021, doi: 10.47059/revistageintec.v11i4.2511.

[7] J. Imgraben, A. Engelbrecht, and K. K. R. Choo, "Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users," Behav. Inf. Technol., 2014, doi: 10.1080/0144929X.2014.934286.

[8] Z. Zhang, X. Chen, J. Ma, and J. Shen, "SLDS: Secure and location-sensitive data sharing scheme for cloud-assisted Cyber-Physical Systems," Futur. Gener. Comput. Syst., 2020, doi: 10.1016/j.future.2018.01.025.

[9] Y. Wang, B. Rawal, and Q. Duan, "Securing Big Data in the Cloud with Integrated Auditing," 2017. doi: 10.1109/SmartCloud.2017.26.

[10] D. Preuveneers, W. Joosen, and E. Ilie-Zudor, "Trustworthy data-driven networked production for customer-centric plants," Ind. Manag. Data Syst., 2017, doi: 10.1108/IMDS-10-2016-0419.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Interrelationship of Cyber Security Issues

Dr. Chellan Kalaiarasan
Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-kalairasan@presidencyuniversity.in

ABSTRACT: ***Innovative technologies allow organizations to remain competitive in the market and increase their profitability. These driving factors have led to the adoption of several emerging technologies and no other trend has created more of an impact than Industry 4.0 in recent years. This is an umbrella term that encompasses several digital technologies that are geared toward automation and data exchange in manufacturing technologies and processes. These include but are not limited to several latest technological developments such as cyber-physical systems, digital twins, the Internet of Things, cloud computing, cognitive computing, and artificial intelligence. Within the context of Industry 4.0, additive manufacturing (AM) is a crucial element.***

KEYWORDS: ***Cyber Security, Cyber Warfare, Industry, Industry 4.0, Organization***

INTRODUCTION

Many of these issues are interdependent and will follow some examples of how they are tied together. The following examples will highlight some of the interrelationships between the issues. Deterrence is something the US uses as a foundational part of its foreign relations policy. There have been many discussions about how this principle can be applied to cyberspace. Before we can begin to utilize it we require attribution pointing to a specific individual, group, or nation that is responsible. If we can solve this, we would still need clear policies on our reaction, military doctrine, and ROE showing our responses. This would not be a simple if a then B equation like the Nuclear Mutually Assured Destruction policy as there is a wide range of factors that could come into play. It would be more like a complex matrix of options which is hard to use as deterrence because the response is often not clear. Military ROE is complex for the same reason deterrence is difficult. There would need to be a clear set of actions with easily understandable reactions preauthorized. National policy, supporting laws, and doctrine would all need to be established. Finally, standards of attribution would need to be determined so commanders could know when they had enough intelligence to act [1].

Mobile devices would require a set of common interfaces to allow system integration. There are so many proprietary systems using unique protocols and configurations that it is not practical or cost-efficient to have one network operations center or security operations center try and manage them all. Some advancement in systems integration is needed to allow the management of all the devices being introduced to networks every year. Audits are becoming critical to risk management, but it depends on developing industry standards. Before these standards can be created, we need to baseline the identity management systems, agree on what metrics will be analyzed, and document the definitions of everything involved.

Stovepipes are tied to the Classification of Data. Stovepipes are organization-based issues but the culture of classification of data is normally set inside the same stovepipe. Once a culture of sharing is established and the walls are broken down the culture of what can reasonably be declassified will allow the release of a lot of information. It is important to note that insider threat is also a key concern when establishing a functional system for sharing information auditing and good identity management both authentication and authorization) are the foundation for building a system that allows the safe sharing of information.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Situational Awareness is the "holy grail" for many large networks. It can mean understanding what the attacker's intent is, what they have done after they got in, how an event has changed the risk posture of the network, what the impact on mission capabilities is, or identifying who it was that penetrated the network. Each of these questions requires a slightly different set of data to answer the question. For some it is just the correlation of the integrated systems, for others it is metrics, some require internal auditing, and a number of them want attribution. The data must facilitate a decision and be presented visually in an intuitive manner [2].

Insider threat needs policy support, auditing, and identity management. First privacy issues need to be addressed. Then we have to find a cost-effective way to track the activity of all users and be able to recognize malicious behavior. Finally, we have to be able to positively identify who took which actions. These must all be solved in a standardized and cost-effective way which requires solving the auditing set of issues and situational awareness issues.

Then there are the issues that involve multiple challenges. To some degree, they are all impacted by a lack of taxonomy, metrics, and standard rules, others are tactical and can be fixed at lower levels while still others require technical innovations for new solutions. Let's look at what level the issues reside at. At the International level, we need agreements and processes to address attribution, supply chain, and legal issues. At the National level, the government needs to set a consistent and interconnected policy/legal strategy, set up governance for standardization of taxonomy and metrics, publish our policy on deterrence, and doctrine, and expand our development of the skilled workforce we need through both training and exercises. To do this we have some organizations that should be the lead for specific missions:

i. Congress would need to set the course for policy and legal statutes and assign/resource many of the roles discussed here.
ii. NIST would focus on taxonomy, metrics, and auditing. They could establish standards for virtualization, cloud computing, data protection, insider threat protection, system integration, and mobile device management.
iii. DOD would develop doctrine with ROE. They would need to build ways to develop a chain of trust and mission assurance for key command and control as well as weapon systems. They require a core of service members with cyberwarrior skills through training and exercises. They are in a good position to address the classification processes and stovepipe issues.
iv. DHS would focus on situational awareness, identity management, IDS/IPS, IPV6 implementation, and dealing with massive data. They would also be the lead for the national program to increase risk awareness and develop the skilled workforce we need.
v. DoS should be the lead for developing deterrence strategies and building international agreements.
vi. DoJ would focus on policy and legal enforcement of the laws we have.
vii. Organizations like Federally Funded Research and Development Centers and Defense Advanced Research Projects Agency would focus on resilience, chain of trust, attribution, and supply chain.

This assignment of challenges is extremely basic and does not represent a clear mapping of the missions of the different agencies/organizations. We have left out players like Whitehouse CIO, CTO, and Cyber Security Coordinator as they don't control significant resources. We didn't include DoE who is working on cybersecurity for smart grid technology. This list was just a sample but reflects some of the intricacy involved with these issues. It is meant to be more of a starting point to allow everyone to weigh in on which issue belongs to which organization. It is clear the current distributed and poorly coordinated effort is not proving to be effective enough to position the US to maintain its current level of influence in cyberspace. We need a national roadmap that assigns responsibility and resources to address these concerns [3].

Another way to categorize these challenges is to look at a rough timeline to solve them. So, with no crystal ball, here is a prediction on some of the issues. In the next 5 years doctrine should be well established based

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

on the current activity in DOD though ROE may not be defined very well. There will also probably be new laws based on the number of bills in Congress. Many technical issues like virtualization, cloud computing, identity management, data protection, massive data analysis, and situational awareness are all being heavily invested in and will see major improvements. Expect to see cyber being included in more exercises and cyber-central exercises becoming more common. IPv6 will force its way onto center stage and become a standard protocol time will tell how much it solves. There are a lot of organizations, both inside the government and commercial that are working on metrics and auditing so we expect major improvements but it is doubtful there will be any global standards established. For those cross-walking all the issues we listed there are some we didn't talk about because we are unclear where they could fit so didn't try and make a prediction.

The US faces multiple challenges today competing for limited resources but only one of them is woven throughout the rest and can be attacked by everyone from a lone individual to a nation-state cyberspace. Several organizations are trying to solve or profit from these issues but there is no critical mass to enable real progress on any of the key issues we have covered in this chapter. The national debate on cyber needs to determine what we must address as many of these issues have a long lead time to solve. We need a leap forward to introduce game-changing technology or change the rules we play by with new policies or even morph the game board by a paradigm shift in the underlying infrastructure of the Internet [4].

The Interrelationship between Additive Manufacturing and Industry 4.0

The fourth industrial revolution called Industry 4.0 named after Germany's Industry 4.0 has made an enormous impact on academia, government policymaking, and industrial sectors. Extensive research is being undertaken to utilize Industry 4.0 for improving business models, product quality, employee skills, communications, and supply chains. Major features of Industry 4.0 are digitization, optimization, and customization of production; automation and adaptation; human-machine interaction; value-added services and businesses, automatic data exchange, and real-time communication. Different countries have different names for Industry 4.0 such as the "Industrial Internet" or "Advanced Manufacturing" in the United States, "Factories of the Future" by the European Commission, and the "Future of Manufacturing" in the United Kingdom. There is no widely accepted definition for Industry 4.0 because of several reasons: no clear framework or boundaries for enabling technologies, rapid innovation of technology and its usage, and differing needs of policymakers, businesses, and academics. Industry 4.0 uses a series of enabling technologies that can be categorized into nine pillars. These are the technologies that have the most applications under the Industry 4.0 umbrella. However, some works have added another pillar known as "other enabling technologies" that have limited applications in agri-foods, bio-based economics, and energy consumption. The ten pillars of Industry 4.0 are shown in Figure 1 [5].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

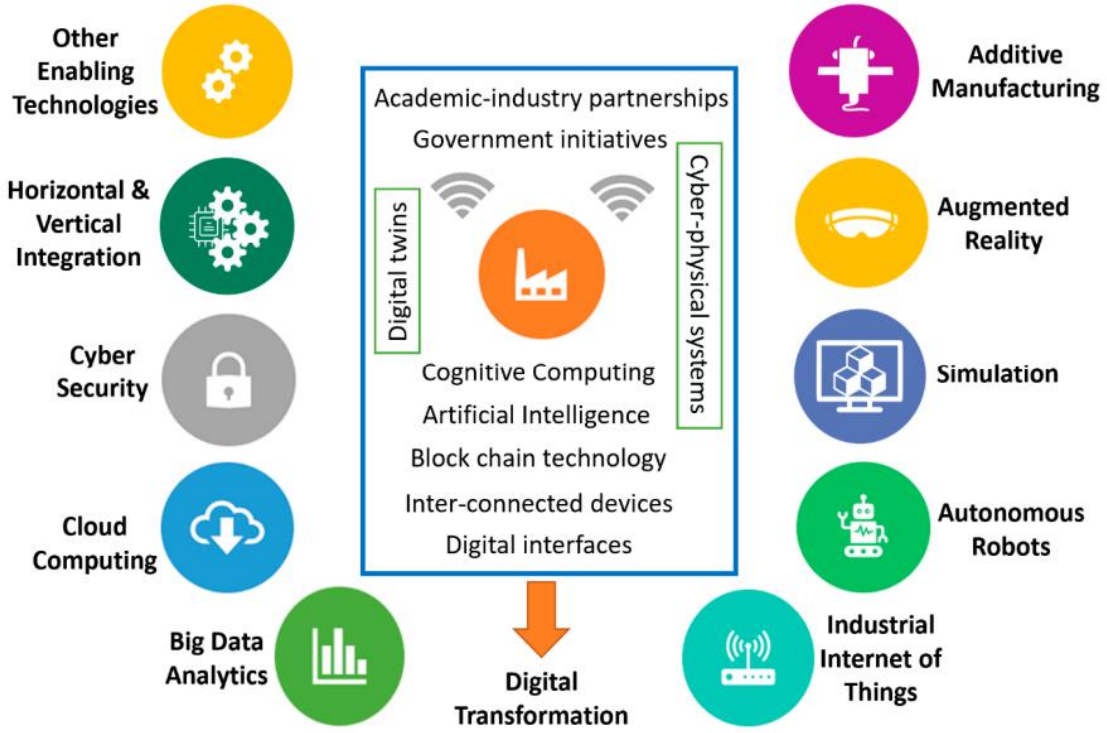

Figure 1: Illustrated the Pillars of Industry 4.0**.**

Industry 4.0 offers several major benefits, but there is a need to accept the lack of readiness from organizations for its implementation. The main challenges that need to be faced before the Industry 4.0 vision become a reality are reducing latencies and ensuring accuracy independent from the physical medium, performing fault tolerance without additional hardware, providing interoperability of solutions from different manufacturers, supporting higher security, safety, and privacy. To combat such barriers, organizations are investing heavily to embrace digitalization. Industry leaders such as General Electric, Siemens, ABB, and Intel are changing their production strategy and management to embrace Industry 4.0. To demonstrate the capabilities of Industry 4.0, MTC from the UK developed a rapidly deployable, remotely managed, modular manufacturing supply chain network enabled by industrial digital technologies called Factory in a Box. This is a rapid route to market for products with a faster return on investment on its manufacturing innovation and new disruptive business models for the supply chain. Government funding bodies are also not far behind and are offering substantial funds for researching different facets of Industry 4.0. A project funded by the European Union titled "GrowIn 4.0" aims to identify barriers to the uptake of Industry 4.0 in SMEs and propose different management-related tools for ease of transformation. Another project funded by the European Union along the same lines is "SME 4.0" which focuses on identifying Industry 4.0 enablers and developing SME-specific strategies and management models. UK government is investing heavily in Industry 4.0-related research through Innovate UK for the development of business models and standards. The United States is also following the same trend with the development of new business models and their quick deployment. On the other hand, the research focus of countries like Japan, Germany, and China is implementing digitalization to increase efficiency and product quality as well as reduce costs [6].

Within the context of Industry 4.0, there are many transformative technologies but there is only one that is associated with a manufacturing operation and is called additive manufacturing. This is an umbrella term that is used to describe techniques capable of manufacturing three-dimensional objects by adding layers on top of each other. The entire operation is digital where a 3D CAD file is sent from a CAD

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

package to a slicing software that creates cross-sections for layer-by-layer manufacture followed by part building. The widely accepted CAD format is STL, but a new format is under development for several years called 3MF that can allow design applications to send full-fidelity 3D models to a mix of other applications, platforms, services, and printers. This is being done for two reasons. The first is to standardize a universal format for AM. The second reason is to overcome the limitations of the STL format which essentially describes a raw, unstructured, triangular surface. In 2015, the 3MF consortium was developed and investigation on this XML-based file format is undergoing ever since. As of 2019, information about material color has been incorporated into 3MF files. The goal is to enable 3MF files to hold more information such as data about more than one object in the scene, printer profile, manually created supports, and variable layer height settings. This format has been adopted by big industrial giants in AM like Materialize, 3D Systems, and Ultimate [7], [8].

AM offers several notable advantages over other manufacturing methods but the most important one is perhaps its ability to manufacture extremely challenging geometries or in some cases impossible to manufacture any other way. Customization and personalization are also benefits that are associated with AM methods which makes it a key technology for Industry 4.0. These aspects also make AM a preferred method for aerospace, automotive, and medical industries. There are seven main categories of AM including vat photopolymerization, powder bed fusion, direct energy deposition, binder jetting, material extrusion, material jetting, and sheet lamination. Working with different raw materials to produce homogeneous and heterogeneous products with highly complex geometries in a time and cost-effective manner are some primary features of AM. Like how Industry 4.0 is moving towards widespread adoption, AM has also passed through that phase. Many roadmaps and reports have been developed, including the NIST roadmap, America Makes roadmap, CSC report, Wohler's reports, etc., to provide industry and business perspectives on AM technologies. With such a wide variety of processes and materials, there exist notable challenges to the implementation of AM as well. They include building scalability, material heterogeneity, structural reliability, skills shortage, intellectual property, and standardization issues. The main recommendation is the cooperation of the research community, industry, and governments to overcome the barriers associated with AM. There should also be a strong focus on university-industry collaboration and technology transfer as well as education and training. This shows a clear need for understanding the role of AM as a pillar for Industry 4.0 and how it fits into the context of the digitalization of manufacturing. This is a major opportunity to complement Industry 4.0 elements in end-to-end digital implementations of AM processes [9].

DISCUSSION

The impact of the fourth industrial revolution, known as Industry 4.0, cannot be denied as it has led to governmental initiatives in addition to academic and industrial research activities. The use of the latest technologies and upskilling of the workforce is vital to staying competitive in the market. The merging of digital and physical worlds has changed manufacturing practices and has led to benefits that were unthinkable a decade ago. This has been made possible because of the implementation of Industry 4.0 practices. However, there are still challenges to be addressed. In addition to the development of digital twins and cyber-physical systems, other aspects also require attention. The primary one is the 5G connectivity. Industry 4.0 is based on a streamlined flow of information from interconnected devices. As the 5G technology develops further and is made available on a wider scale, it will significantly accelerate Industry 4.0 protocols [10], [11].

CONCLUSION

Much like the adoption route taken by Industry 4.0, one of its pillars i.e., additive manufacturing has been through a similar trajectory starting from prototyping and visualization in the 1980s to customization and mass production in the 2020s, and still growing in demand. AM is still a widely researched area and future developments will lead to more applications in different industrial sectors. It has strong ties to all the other pillars of Industry 4.0 whether they can be used directly or indirectly. With the development of new machine learning and artificial intelligence protocols, the benefits offered by AM will continue to grow with the efficient processing of data for process and product improvements. This paper has provided an in-depth literature review of the interrelationship between Industry 4.0 pillars and AM. It highlights the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

importance of AM in the context of Industry 4.0 and the need for continuous development to shift towards smart manufacturing. The use of AR provides an interactive experience and is quickly being adopted in different industrial sectors to aid operations. However, its use for detecting inter-layer defects in AM requires more sophisticated protocols. Simulation has been a useful tool for AM but is often limited without experimental validation to achieve reliable results. The use of new technologies requires integration activities to ensure seamless operation as highlighted in Section 2.3 with autonomous robots. The data collated through IIoT require processing through BDA and a couple of major AM-specific limitations are topology optimization of products and the development of lattice structures.

REFERENCES

[1] Z. Rashid, U. Noor, and J. Altmann, "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem," Futur. Gener. Comput. Syst., 2021, doi: 10.1016/j.future.2021.05.033.

[2] R. Rajan, N. P. Rana, N. Parameswar, S. Dhir, Sushil, and Y. K. Dwivedi, "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management," Technol. Forecast. Soc. Change, 2021, doi: 10.1016/j.techfore.2021.120872.

[3] O. V. Sviatun, O. V. Goncharuk, R. Chernysh, O. Kuzmenko, and I. V. Kozych, "Combating cybercrime: Economic and legal aspects," WSEAS Trans. Bus. Econ., 2021, doi: 10.37394/23207.2021.18.72.

[4] Y. M. Bogdanov, A. L. Ogarok, and S. A. Selivanov, "Monitoring cybersecurity of complex Information and control systems of critical Infrastructure," Informatiz. Commun., 2021, doi: 10.34219/2078-8320-2021-12-1-142-150.

[5] M. Ghobakhloo, "Determinants of information and digital technology implementation for smart manufacturing," Int. J. Prod. Res., 2020, doi: 10.1080/00207543.2019.1630775.

[6] "Architecting A Cybersecurity Mangement Framework," Issues Inf. Syst., 2016, doi: 10.48009/4_iis_2016_227-236.

[7] "Cybersecurity: Challenges From A Systems, Complexity, Knowledge Management and Business Intelligence Perspective," Issues Inf. Syst., 2015, doi: 10.48009/3_iis_2015_191-198.

[8] B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," Rev. Fac. Ing., 2018, doi: 10.19053/01211129.v27.n47.2018.7807.

[9] S. H. Jore, "The Conceptual and Scientific Demarcation of Security in Contrast to Safety," Eur. J. Secur. Res., 2019, doi: 10.1007/s41125-017-0021-9.

[10] B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," Rev. Fac. Ing., 2018, doi: 10.19053/01211129.v27.n47.2018.7808.

[11] Z. Rashid, U. Noor, and J. Altmann, "Network externalities in cybersecurity information sharing ecosystems," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019. doi: 10.1007/978-3-030-13342-9_10.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Introduction to Cyber Warfare Headed in Cyber Security

Ms. Sandhya Kaipa
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-kaipa.sandhya@presidencyuniversity.in

ABSTRACT: ***Cyberwar also spelled cyber war, also called cyberwarfare or cyber warfare, is war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks to disrupt, destroy, or deny their use. Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.***

KEYWORDS: ***Cyber Warfare, Cyber Security, Computer Science, Information Technology, and Military Technology.***

INTRODUCTION

Technology has had impacts on warfare throughout history. Some caused a "Revolution in Military Affairs", also known as "Military Technical Revolutions," like gunpowder, nuclear bombs, and space platforms. Others have caused paradigm shifts in organizational structures and doctrine such as airplanes, submarines, and machineguns. Some innovations have been transformational like stirrups, precision strike munitions, and radios. Some inventions were designed for the military while others like internal combustion engines, railways, and information technology advances were leveraged by it. Some of these changes were incremental like the machine gun being a natural change to increase the rate of fire for rifles. Others reflect the concept of Black Swans or Dragon Kings where there was dramatic surprise about the change. Cyber warfare has transformed all these aspects of change [1].

Cyber warfare has changed to what has been called, including Electronic Warfare, Information Superiority, Information Dominance, Network Centric Warfare, Information Warfare, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance, Hyper war, NetWare, and Third Wave Warfare. These terms generally refer to conflicts in the cyber domain. Cyber is separate from other RMAs ongoing today in unmanned aerial vehicles, nanotechnology, robotics, and biotechnology. Cyber is built on a physical infrastructure but is unique in that it has a virtual component. It also is prone to more rapid shifts since the software is developed at a much faster pace than hardware. Technology will continue to drive change in society, economies, and warfare. We will start by looking at some of the changes that have impacted the Internet in general [2].

As a baseline, we have provided a timeline of the major cyber events along the cyber timeline. This is a good format to look for paradigm shifts in both security and threats as well as where we seem to be stuck in a paradox experiencing the same issues year after year. We will see that while at the time of an event many of us believed it to be significant, many seem to have had no long-term impact. There are some major evolutionary events and a few with revolutionary impacts. As a sample, we would point to 1988 when the Morris worm should have been a wake-up call for security, but in 1999 we see the same thing when the Melissa virus hit, then again in 2004 when Love Letter caused havoc. These show a pattern of the military and the IT industry ignoring the fundamental security issues that allowed these worms and viruses to spread. Some major events in cyber conflicts are the 2004 SCADA attack on the Russian pipeline, the 2007 attacks on Estonia, the 2008 Buckshot Yankee intrusions, and the cyber-attacks against Georgia during the conflict with Russia. In 2010 we had Operation Aurora against Google and StuXnet SCADA attacks. These events show an increasing use of cyber-attacks with overtones of state sponsorship. In the revolutionary category, ARPANET is being

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

stood up and social media exploding onto the net. These were events that created paradigm shifts in how we use the Internet and open up net threat vectors at the same time. As we look at the potential threats, one way to categorize them is by the level of resources they commit [3].

Critical Infrastructure in the Age of Cyber War" executives from many nations, including many US allies, rank the United States as the country "of greatest concern" in the context of foreign cyber-attacks, just ahead of China. At the next level, there are countries and non-nation state actors like criminal organizations investing millions of dollars in developing and employing cyber tools. Finally, there are individual hackers or groups like Anonymous that only spend thousands of dollars. Unfortunately, unlike conventional weapons development, the potential impact of these organizations can't be based on their resources alone. That said we will continue to see rapid increases in attack capability, many of which are designed to be stealth or classified [4].

Another way to categorize potential threats is how they impact aspects of national power. These would be based on evaluating the impact of attack defend exploit capabilities across Diplomatic, Information, Military, and Economic elements of national power. Typically, discussions on warfare focus on armies, weapons, and leadership but in today's conflicts, we are seeing more integration of all these capabilities. The US Secretary of Defense is talking about both cyber and the national debt today. DIME presents a solid way to evaluate the multiple aspects of Internet-based activities that can be part of cyber warfare. The impact of intellectual property theft can be looked at as economic warfare when you consider the aggregated damage to a nation but what about the impact of cybercrime? This chapter will review where cyber warfare is going based on these elements, but in the end, we must devise a national formula that will ensure we are ready for the next conflict based on something like the Aggregation of:

Capabilities + Innovations + Resources + Leadership = Strategic Advantage.

Technology-Based Trends

The first technology that is changing the virtual landscape is cloud computing. For most companies running a network is a distraction and at some point, it is natural to outsource tasks that are not part of the core business. Looking at a historical example of this, in the early days of electrical energy, manufacturing plants would run their power plants, but as a common power grid became more reliable they eventually decided to move to it and go back to focusing on their core business. We are approaching that tipping point in the next few years with corporate networks and cloud computing where we see companies shift the capability to an external service with high expectations of reliability. As the cost, security, and reliability of cloud computing continue to increase it will become standard to get rid of the distraction of managing internal networks and outsourcing to the cloud. Use of the cloud will still need strong corporate governance and for some organizations just a few years ago it would never have been considered an acceptable risk, but today for most it will become standard. There are security advantages and disadvantages but again it is important to remember that the threat will target the place they can gain the most advantage or impact. Botnet builders love the idea of consolidating resources into one target; compromising one cloud provider would give them an instant botnet army. The Advanced Persistent Threat today has to break into multiple systems to find the information they are after; they also would love one target that has all the desired information. The military and critical infrastructures are moving to the cloud and it will impact the cyber landscape [5].

Another key issue is the number of mobile devices users are connecting to our networks so they can do their work and manage their personal life at the same time. People have laptops, smartphones, thumb drives and tablets to be more productive and few users think about security when they are using these mobile devices. Many users download applications to all these devices with no concern about the security or validity of the programs. There are also a lot of devices that are not necessarily mobile but are becoming connected to the Internet. Our cars can be remotely tracked, our houses will soon be able to be monitored to track our activities as our heating system and refrigerators become connected. While we think of the advantages, the threat is busy thinking of new "business models" to take advantage of them. If we are mad at our neighbor we can turn off their heating system when they leave for work in the winter. If we want to sell more tune ups we can remotely turn on the check engine light in the cars that use our garage. If we want to sell information on the people who live in Colorado Springs we can track their electricity usage and sell the information to companies that sell solar panels so they would know their best potential sales targets.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Conversely, as Colorado Springs has five military forts/bases, you can track activity of both the installations and potentially key leaders based on energy consumption or other embedded devices [6].

Situational Awareness and Visualization are based on the correlation and fusion of data from multiple sources that enable decision making that is presented in an intuitive way to the units' leadership. Situational Awareness consists of functions like Continuous Monitoring, Security Information and Event Management for correlation, Common Operational Picture for relevancy, and a Dashboard for visualization. Most of the current COPs / Dashboards fail to facilitate true risk posture understanding and provide information in a format that enables decisions. There are processes like the situation awareness global assessment technique, situational awareness rating technique, and situation present awareness measurement that provide useful processes. The military needs to be able to understand both the impact of enterprise risk posture and the mission capabilities of a network security event.

The number of Internet Protocol v4 addresses is running out quickly forcing new Internet sites to use IPv6. It is predicted, at the time of this writing, that there will be no more available within the next 18 months. As the Web pages on the Internet are divided into IPv4 vs. IPv6 there will be many security issues including no longer needing Network Address Translation to extend IP addresses which will open up entire networks to discovery. Also, most security tools we use today are not designed to operate over IPv6, and currently only a few skilled administrators and a limited number of vendors support IPv6. However, IPv6 has benefits such as, hacker scanning will become problematic as address space will be so much larger, Internet Protocol Security Encapsulating Security Payload is designed-in, IPsec Authentication Header is embedded as well, we can have virtual private networks without tunnels and there is enhanced routing security. Countries like China are aggressively deploying IPv6 and will be ahead of the curve, which could give them a strategic advantage in capabilities and developing international standards. This change has been predicted for some time and it is hard to tell when we will hit the tipping point to move the majority of Web sites to IPv6.

Bring Your Device as the military and other organizations allow increasing numbers of employees to bring their personally owned devices to work, it will become more complex to implement enterprise security solutions. Allowing devices like data-enabled phones, iPads, and laptops with different operating systems reduces cost of infrastructure but introduces more risk to security. Dale Meyer rose points out this has been happening for years so in some ways this acknowledgment of the practice could increase overall security. Soldiers are taking these devices onto the battlefield today. The impact to the military is now mission-critical data could be on personal devices which are not under enterprise security.

Even if we do secure our networks we have "social networking" activities that open attack vectors that bypass our network security infrastructure. Most organizations are not putting the effort into training their staff on how to practice due care or diligence when on places like Facebook and Twitter so we believe this issue will continue to grow. The Air Force has put out an official policy on how to interact with social media as airmen posting about activities within a combat theater of operations could reveal mission-sensitive information [7] .

As the military considers threats to their capabilities, their reliance on publicly owned energy providers has started to be analyzed. Often referred to as Critical Infrastructure Protection /Industrial control system /Supervisory Control And Data Acquisition issues, the military has undertaken a program called Smart Power Infrastructure Demonstration for Energy Reliability and Security to make military installations energy self-sufficient. On the commercial side, Jim Brenton, a Principal Regional Security Coordinator for the Electric Reliability Council of Texas, talked about both the recent improvements driven by the North American Electric Reliability Corporation CIP program and the energy sector's natural focus on reliability that is tested continuously by different extreme weather events around the country. All of the different critical infrastructures will continue to grow in importance as part of cyber conflicts.

Attack vector trends will continue to follow the most popular applications. As the use of email grew, the threat used it to gain access. Today that is happening with social media and mobile devices. As we move forward there will naturally be new vectors for attack, some technical, others procedural but always following the latest technology trends as they normally have initially immature security built in. Some good companies to follow to stay current are I Defense, Force, Dambala, iSight, and the annual CSI Computer Crime and Security Survey.

Cyber weapons like StuXnet and Flame will continue

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

to become more complex and capable. We will see more public doctrine and legal definitions built around the concept of cyber weapons. The US is investing in the development of these capabilities through projects like Plan X developed by the Defense Advanced Research Projects Agency where "the Pentagon is turning to the private sector, universities, and even computer-game companies as part of an ambitious effort to develop technologies to improve its cyber warfare capabilities, launch effective attacks, and withstand the likely retaliation ." Expect the use of cyber weapons to continue to grow and become more categorized as to their level of impact which will be tied to the release authority.

A couple of new items of security interest are biometric and nanotechnology trends. The trend toward biometrics is going to lead to new threats as their use grows. First, there are no governing statutes protecting our biometric data today. Second, biometrics is not a silver bullet—the threat will eventually find ways to compromise it. Finally, as we field these systems we will need to build analytics and security integrated into the design. If we use biometrics we need to ensure it has been reviewed by folks who think like malicious hackers instead of engineers who think about how to make things work. The second is nanotechnology where generally devices are sized from 1 to 100 nm. These devices can swarm to accomplish more complex tasks. The concerns revolve around building security into the devices upfront and losing control of the devices as they morph into new capabilities.

One final evolution to be considered is the change developing in defensive Security Operations Centers. Initially, these incident response centers were focused on manually reviewing logs or output from standalone systems like Intrusions Detection Systems. Next, they started correlating across multiple security devices to identify attacks. Now we are seeing a move toward what the military calls all-source intelligence where multiple types of intelligence feeds are integrated with a fusion cell. The new SOC will continue to drive toward the goal of predictive analysis but will need to take feeds from traditional Security Information and Event Management solutions and be able to integrate information from feeds like social media, cyber threat intelligence services, and user input. One example where this has been enabled was when the US had a single commander over both NSA and CyberCom facilitating collaboration across the two organizations [8].

Policy-Based Trends

There is an ongoing debate about whether there is a cyber war being waged today. There are two sides to the argument. On the "cyber Armageddon" side the spokesperson is Mike McConnell, former Director of National Intelligence and currently a Senior Executive for a defense contractor, who wrote in the Washington Post "The United States is fighting a cyberwar today, and we are losing. It's that simple." On the "cyber war is hype" side Bruce Schneider wrote a Cable News Network piece saying "We surely need to improve our cybersecurity. But words have meaning and metaphors matter. There's a power struggle going on for control of our nation's cybersecurity strategy, and the National Security Agency and the Department of Defense are winning. If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of "war," we feed our fear. If, on the other hand, we use the more measured language of cybercrime, we change the debate. Crime fighting requires both resolve and resources, but it's done within the context of normal life. We willingly give our police extraordinary powers of investigation and arrest, but we temper these powers with a judicial system and legal protections for citizens." These arguments need to be weighed as they will determine how we approach and solve the cyber conflicts of today.

As we look at the progress achieved over the last couple of years there are two reports worth reviewing. The first is a report "Cybersecurity Two Years Later" by the Center for Strategic International Studies commission on cybersecurity for the 44th Presidency. It is a review of progress on the commission's original recommendations. Under the section "Prospects for Cybersecurity 2012" it states "Our review of the last 2 years found that there has been progress in almost all of the areas we identify as critical, but in no area has this progress been sufficient. The cybersecurity debate is stuck. Many of the solutions still advocated for cybersecurity are well past their sell-by date. Public-private partnerships, information sharing, and self-regulation, are remedies we have tried for more than a decade without success. We need new concepts and new strategies if we are to reduce the risks in cyberspace to the United States." The second report is from a lesser known organization called National Security Cyberspace Institute called "Cybersecurity Report Card." It gave the Obama administration very average grades and most of the concern was on lack of timely progress on the goals set out in the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Cybersecurity Report Card. Both of these reports stress that while we are making progress it is very slow.

There is also an economic warfare aspect to what we are facing. In some ways, the major cyber catastrophe that many newspapers predict has happened with the amount of data that has been stolen from militaries, governments, critical infrastructures, and commercial companies. The loss of Intellectual Property is hard to measure and determine the scope of damage but attacks are rampant. One estimate put US losses of intellectual property and technology through cyber espionage at $240 billion. An estimate of German losses of intellectual property due to cyber espionage puts them at perhaps $20 billion. Cybercrime is the second half of the economic equation. These two issues are eroding the economic power base the G8 countries like the United States enjoy today. Finally, former Chairman of the Joint Chiefs of Staff, Adm. Mike Mullen, observed that one of the greatest threats to national security is our national debt. This means the amount of money we can spend to improve cyber defensive capabilities will come under increasing pressure and many programs in both the military and broader government may be delayed or canceled [9].

We don't teach other countries how to build atomic bombs in our universities but we do teach them everything we know about cyberspace. Most products related to cyber are not actively controlled by International Traffic in Arms Regulations as we don't have clear rules about what constitutes an export of a cyber capability that can be used as a weapon. As the government has moved from driving technology to buying it they are now using standard commercial-off-the-shelf products many of which were programmed and built all around the world. Much of the research is now also being done overseas. So as we continue to realize and talk about how critical the cyber domain is to our national interests and what a central role it will play in any kind of conflict we are aggressively exporting everything about it.

The legal landscape for cyber is moving in two parallel directions today. First is the idea that private lawsuits will drive public law. The second is that Congress will enact laws to protect aspects of national critical infrastructure, privacy, and intellectual property. There are several lawsuits and legislative initiatives ongoing today and there is no clear trend on what guiding principles will come from them. At the same time, commercial companies are offering cyber services to support the military and Law Enforcement Agencies to the point many organizations are outsourcing what was traditionally thought of as government employee-only work because of the lack of skills within the military. At the end of the day, this is an international issue. Because the United States and China have developed technological capabilities in the cyber arena, the nations must work together to avoid misperceptions that could lead to a crisis, according to Defense Secretary Leon E. Panetta.

As we look at the leadership of most organizations today there is what we call the "wristwatch syndrome." Most of the people making decisions today were not raised around computers and think of them as support devices, not as the primary means of accomplishing the mission. They still wear their watch even though they have the time available on their cell phone because they have always worn a watch and don't need to change it. The younger generation has never worn a watch and many have never had a camera that used film or know how to use a paper map. One of the authors was at a simulation exercise and asked a young airman what they would do if they lost the network in the command center and was told, "We couldn't fly anymore." For the generation of military personnel who used grease pencils to track the movement of entire divisions, this attitude was unthinkable. So the baby boomers who are in charge today they many times don't think in terms of risk to the mission when talking about the network. When the digital native generation takes over leadership of the terror groups plotting to attack the West they will default to remote attacks trying to use our mission control systems and critical infrastructure to be the central point of attack rather than a supporting function [10].

DISCUSSION

We have heard the term "Sputnik moment" on the political stage lately. One of the institutions that came out of America's reaction to "losing the race to space" was DARPA. DARPA has a cyber thrust designed to enable military systems and infrastructure to operate effectively in the presence of cyber-attacks. Technologies that eliminate entire classes of vulnerabilities, that adapt immediately to evolutions or novel developments of the cyber threat, and that raise the cost of employing cyber technologies against US forces are the focus of this thrust. Also, of interest are approaches to the development of cyber-based intelligence, surveillance and reconnaissance

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

capabilities, the integration of cyber technologies with communications and electronic warfare systems, and the leverage of commercial advances with cyber technologies. They have many programs ongoing to include: Cyber Genome, Dynamic Quarantine of Computer-based Worm Attacks, Military Networking Protocol, National Cyber Range, Scalable Network Monitoring, Quantum Computing, Cyber Trust program, and Cyber Insider Threat. These programs are aimed at keeping the US's technological edge. The question is, are they funded and able to move fast enough to do it?

CONCLUSION

There is a strong trend toward mergers and acquisitions in the cyber market. A few examples of this trend are HP acquired Arc Sight, Fortify, and Tipping Point to provide integrated cyber solutions. RSA acquired Net Witness, Archer, envision, and Green Plum so they could provide single enterprise cybersecurity solutions as well. Intel acquired Symantec to expand its product's capability. IBM has acquired a host of analytics companies focused on cyber and big data capabilities. Defense contracts like ManTech have expanded cyber capabilities by acquiring companies like HBGary or in the case of Kato who acquired Secure Info and RTLogic gain access into the cyber market. What is not clear is the impact of this trend. It could lead to a lack of open security solutions as more pure security companies disappear and their capabilities are offered as part of a larger package from a company or it could lead to better security products as the larger companies put more resources into growing the capabilities of the companies they have acquired. Finally, as young cyber companies are acquired it reduces the possibility of the next Microsoft/Google/Facebook size company from impacting the security market in unexpected ways.

REFERENCES

[1] K. Nettis, "Multi-Domain Operations: Bridging the Gaps for Dominance," Sixt. Air Force (Air Forces Cyber), 2020.

[2] S. Winterfeld, "Where is Cyber Warfare Headed?," in The Basics of Cyber Warfare, 2013. doi: 10.1016/b978-0-12-404737-2.00009-4.

[3] A. F. Krepinevich, "Cyber Warfare: A 'Nuclear option' ?," Cyber Warf., 2012.

[4] J. Fritz, "How China will use cyber warfare to leapfrog in military competitiveness," Cult. Mandala Bull. Cent. …, 2008.

[5] M. Knopová and E. Knopová, "The Third World War? In The Cyberspace. Cyber Warfare in the Middle East.," Acta Inform. Pragensia, 2014, doi: 10.18267/j.aip.33.

[6] M. Murphy, "Cyberwar: War in the fifth domain," Econ., 2010.

[7] G. Baram, "The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case," Mil. Strateg. Aff., 2013.

[8] A. Rathmell, "Cyber-terrorism: The shape of future conflict?," RUSI J., 1997, doi: 10.1080/03071849708446185.

[9] B. Dalton and N. Agarwal, "Analyzing deviant behaviors on social media using cyber forensics-based methodologies," 2017. doi: 10.1109/CNS.2016.7860520.

[10] R. D. Delpizzo, E. R. Reinhardt, J. Hong, and S. Valluri, "Evolution of worldwide naval design and standardization," 2017.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Introduction to Action Threats and Challenges in Cyber Warfare

Mr. Budden Asif Mohamed
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-asif.mohamed@presidencyuniversity.in

ABSTRACT: ***Cyber warfare is arguably at the most serious end of the spectrum of security challenges posed by and within cyberspace. Just like the tools of conventional warfare, cyber technology can be used to attack the machinery of the state, financial institutions, the national energy and transport infrastructure, and public morale. However, while some actions may appear aggressive and warlike, they may not necessarily be intended as acts of war. It is important, therefore, to distinguish between warfare and non-warfare in cyberspace. It is the action and its warlike properties that matter as much as the actor. For example, the cyber actions of terrorist groups, spies, and organized criminals can be harmful and appear aggressive but they do not in themselves necessarily constitute acts of cyber warfare.***

KEYWORDS: ***Cyber Security, Cyber Threats, Computer Virus, Cyber Warfare, Internet.***

INTRODUCTION

Despite growing recognition of the scale and nature of threats emanating from cyberspace, the virtual world remains largely uncharted and little understood. Threats within and from it are disparate, diffuse, and disproportionate in the harm they could cause. Moreover, unlike in conventional attacks where the perpetrator is usually physical and identifiable, the attacker in cyberspace can be virtual and anonymous. Differentiating between actors with 'warlike' intentions and those who are merely malicious or criminal and whose actions fall short of 'acts of war' is therefore problematic. Yet distinctions can and should be made to ensure effective and appropriate responses. Taking a thematic rather than an anecdotal approach, in this chapter we use a conventional analysis of warfare to reveal the characteristics of the cyber variant. What is the source of direct and indirect security threats in and from cyberspace? Who, or what, are the main actors? What is the actor's intent: are his actions motivated by a desire to dominate, gain a political or strategic advantage or cause substantial harm to a state or a population in pursuit of personal financial gain or self-interest? We also seek to identify the challenges which are distinctive and unique to cyber warfare. Is it reasonable to describe all incidents of cyber aggression as 'warlike'? What are the politics which shape an actor's behavior in cyberspace? How easy is it to distinguish cyber warfare not only from other cyber security challenges but also from other forms of conflict? [1]

Threats

The character of conflict in cyberspace is as diverse as the actors who exploit it, the actions they take, and the targets they attack. Cyber targets can be found not only within the state apparatus or the armed forces but also – just as in physical warfare – in the economic, environmental, and social domains. The discussion of actions and actors in this chapter is loosely based on the four cyber threat domains identified in the March 2009 Chatham House report: state-sponsored cyber-attacks, ideological and political extremism, serious organized crime, and lower-level/individual crime.11 These domains provide a useful framework, although we will show that the asymmetries of cyberspace enable a range of other actors, and not just states, to use virtual means, in some cases with a psychological dimension, for their hostile ends. We do not suggest, either, that all hostile actions in cyberspace must fit into one or more of these categories: we could envisage, for example, 'cyber protest' whereby a nuclear facility of some sort is attacked for ecological reasons. In many cases, the actions we describe have all the appearance of warlike activity. But often the distinction between what is and what is not warlike is blurred and there are inevitable exceptions to any rule.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Hostile actors in cyberspace can make use of a wide range of techniques. Malicious software (malware), networks of 'botnets', and logic bombs can all be employed to navigate target systems, retrieve sensitive data or overrule command-and-control systems. Yet although the technology and skills involved in designing, building, testing, and storing these weapons may be complex and advanced, how the weapon is delivered and by which the desired damaging effect is caused may be very basic (if very cunning). One well-known example occurred in 2008 when highly classified US Department of Defense networks were infected by an unknown adversary that 'placed malicious code on USB thumb drives and then dispersed them (in parking lots) near sensitive national security facilities. After a curious finder inserted the drives into computers, the code spread across their networks.' Simple actions of this sort which can nevertheless have a dramatic effect would be described in military terms as an 'asymmetric' attack: asymmetry seems to be characteristic of much hostile action in cyberspace. We begin our analysis of cyber warfare at the level of the direct military threat [2].

Direct Military Threats

Cyber technology has clear military applications which can be exploited in conflict situations. Whether through military equipment and weapons systems, satellite and communications networks, or intelligence data, armed forces are highly dependent on information and communications technology: 'For the top brass, computer technology is both a blessing and a curse. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data processing centers; even the ordinary foot soldier is being wired up. In a digital, knowledge-based society this is to be expected. But while technology brings opportunities it can also create vulnerabilities. The People's Republic of China (PRC), in particular, has long recognized the strategic and tactical value of cyberspace. Unable to match the current military superiority of the United States in terms of its military and technical hardware, the PRC has countered this asymmetry by developing its cyber capabilities: 'Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict [3].

To offset its conventional weakness the PRC is transforming its armed forces 'from a mechanized to an "information zed" force and have stated they intend to use information "as a tool of war or as a way to achieve victory without war"'. To date, the PRC's focus has been on 'active defense' in preparation to counter aggression. Questions might be asked about the PRC's perceived methods principally espionage and network infiltrations and whether 'active defense' might more accurately be described as 'pre-emptive attack', where such actions may be preparing the ground for a future, more overt act of aggression. Russia has also recognized the importance of cyber capabilities. In both Estonia in 2007 and Georgia in 2008, Russia is alleged to have used cyber technology as part of a 'coordinated and synchronized kinetic and non-kinetic campaign'18 through distributed denial of service (DDOS) attacks which appeared to be orchestrated with military and political operations. While both states deny the actions they are alleged to have committed, the use of cyber capabilities in conjunction with a conventional military campaign seems likely to be a feature of future warfare between states.

Indirect and Non-military Threats

Just as the targets of physical warfare are the machinery of the state, financial institutions, the national energy and transport infrastructure, and public morale, so too are they the prime targets in cyber warfare. One of the earliest recorded cyber-attacks on national infrastructure occurred during the Cold War when US President Ronald Reagan approved a SCADA (supervisory control and data acquisition) attack on the Russian pipeline system in Siberia in 1982. In 2004 Thomas Reed, who had been Reagan's Secretary of the Air Force, described the incident in the following way: 'The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds.' One of the earliest examples of a 'logic bomb', this attack was part of a broader, indirect effort by the US to disrupt the Soviet Union's technological capabilities and military industrial base. In the context of Cold War tensions, the pipeline attack was specifically designed to disrupt the Soviet Union's gas supply and harm the Russian economy and its gas revenues from the West, thus undermining its power [4].

In a more recent attack, the 'Stuxnet' worm was infiltrated through the 'back door' of IT systems and used a number of 'zero-day' exploits (previously unknown vulnerabilities) in an attack believed to have

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

been aimed at the industrial control systems at the Bushehr nuclear reactor or the Natanz uranium enrichment plant in Iran a politically valuable target, particularly given pressures on Iran to halt its uranium enrichment program. This sophisticated SCADA attack demonstrated the potential of future cyber-attacks and cyber warfare. Yet it also revealed its limitations of such attacks, not least the porous borders of cyberspace which led to the infection of thousands of additional computers both in Iran and beyond. The Russian pipeline and the Stuxnet incidents both reveal the potential of attacks to exploit vulnerabilities in civilian infrastructure and bypass military involvement. If the allegations are accurate, the actors concerned were able to achieve political and strategic effect without the need for armed conflict. The lack of clear attribution and the almost remote and indirect nature of the cyber-attacks, which in both instances took time to uncover, made retaliation difficult without the risk of political controversy and, at worst, disproportionate damage.

Although attacks upon infrastructure occur in conventional warfare, the implications are very different in cyber-space. As Lord West, former UK Minister for Security, once commented: 'If I went and bombed a power station in France, that would be an act of war but if I went on to the net and took out a power station, is that an act of war? One could argue that it was. These boundaries remain unclear but they pose important questions about the relationship between the civilian and military domains in the context of cyber warfare and the role and involvement of the armed forces in such undertakings.

Terrorism and Extremism

As for organized criminals, the asymmetries of cyberspace and its hidden depths can be a valuable resource for non-state actors such as terrorist and extremist organizations. Although there is no conclusive evidence certainly in the public domain that groups such as Al-Qaeda have the capabilities or resources yet to launch a major cyber-attack, terrorist groups are increasingly web-literate and use the internet and deep web in order to propagate their message and mobilize supporters. The internet has brought disparate groups together and facilitated conflict by enabling militants and extremists to share techniques, spread their message, recruit foot-soldiers and highlight their successes. Moreover, the evolution and democratization of technology have enabled sophisticated but relatively cheap everyday items such as smart phones, online mapping and the internet infrastructure to be used as vital operational components of conflict in conjunction with conventional methods.

The potential applications of communications networks, mobile information systems and intelligent technology in facilitating terrorist attacks were all in evidence during the Mumbai bombings of November 2008 when terrorists (Lashkar-e-Taiba) used GPS systems and 3G smartphones, alongside conventional weapons, to prepare for and carry out attacks on civilian targets. In this case the technology was used in a relatively rudimentary manner, recording and detailing reconnaissance information on the targets, enabling communication between the perpetrators and providing tactical guidance to the gunmen during the attack [5].

Cyber Espionage

Cyber espionage is one of the most prevalent of cyber activities. Whether used to uncover sensitive government information, steal trade secrets or commercial data or as part of intelligence or reconnaissance work, it fits into the doctrine of using 'information superiority to achieve greater victories at a smaller cost'. As Eleanor Keymer has observed, 'the return on investment for targeting sensitive information can be extremely high compared to the skills and technology required to penetrate the system which are relatively low'. Although China, unlike Russia, has not yet been linked to attacks connected to conventional military activity, it has employed cyber espionage to great effect to penetrate military, government and industrial targets to gather sensitive information. The Titan Rain attacks in 2007 one of the most large-scale infiltrations of US and UK government departments, including the US Department of Defense and the UK Foreign and Commonwealth Office were attributed to China, and had allegedly been under way since 2002. Furthermore, in March 2009 China was linked to 'Ghost Net' when it was revealed that a large-scale spying network had attacked a significant number of government departments and strategic targets, including the Tibetan community. In the words of the Information Warfare Monitor, the Ghost Net affair 'demonstrates the ease by which computer-based malware can be used to build a robust, low-cost intelligence capability and infect a network of potentially high-value targets'.30 States are not the only targets: defense companies, commercial

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

companies (such as Google) and NGOs have also been affected by cyber espionage.

However, it would be incorrect to assume that espionage or the infiltration of networks by malign actors constitute cyber warfare in their own right. Espionage is arguably a long-established feature of the physical world a balanced friction. Its encroachment into cyber networks is therefore, in part, an extension of this tacitly condoned activity. While this may not make it right or any less concerning, cyber espionage may in many ways be a different means to a well-known end, and not necessarily a radically new threat. Nonetheless, as with the nature of this threat, little is known about its current or future potential. What happens, in other words, when this 'balanced friction' in cyberspace is disturbed? In particular, there is growing awareness of the ability of aggressors to use espionage and infiltration to plant 'back doors', Trojan horses and logic bombs which can remain dormant and undetected until time and circumstance require. Once activated, these time bombs would enable an aggressor to rapidly take control of a targeted system before the victim has become aware of either the intruder or the infiltration. These virtual attacks, if coordinated, could unleash significant damage at a designated time, either at a point of political tension or as an accompaniment to conventional warfare.

Economic Cyber Crime

There is increasing potential for financial institutions to be the target of digital attacks. This normally constitutes cybercrime, described by the UK Home Office as actions 'undertaken by serious organized criminals, who target government, business and the public to obtain money or goods. Their motivation is largely for financial gain, but it can also be to inflict personal harm. It appears to be organized criminals who are engaged in such attacks on financial institutions and these could not plausibly be described as 'acts of war'. Yet when these attacks are persistent and insidious, they could arguably pose a risk to the national balance sheet and be detrimental to industry and society as a whole, consequently affecting the security and stability of a state. According to the UK's National Security Strategy 2010, 'cyber-crime has been estimated to cost as much as $1 trillion per year globally, with untold human cost'[6].

At what point do such actions become another form of warfare? Or should they remain the preserve and responsibility of financial institutions and their customers? We would argue that given the potential costs to a single nation-state, economic cybercrime should not remain the concern of the financial industry alone and combating it should indeed be incorporated into national strategy, as in the case of the United Kingdom. A further consideration is that cyber-crime provides an environment in which attack techniques can be refined. In the words of Jeffrey Car, 'cyber-crime is the laboratory where the malicious payloads and exploits used in cyber warfare are developed, tested and refined'. This further underlines the interconnectedness of attacks, where actors and agents are not uniform and clear cut but operate within a murky world where it is hard to identify the perpetrators in any given case.

Psychological Cyber Warfare

There can be a psychological dimension to cyber-attacks. The infiltration of what are assumed to be secure systems and critical infrastructure highlights national vulnerabilities and weaknesses. This can provoke feelings of insecurity, as evidenced by the Stuxnet worm in Iran and the Titan Rain episodes in the United States and the United Kingdom. Engendering this sense of insecurity could indeed be the attacker's goal, in the same way that the fear of terrorism and its potential harm can have a detrimental and disabling effect almost as great as the terrorist act itself. Indeed, according to Dennis Murphy, 'some observers equated that cyber-attack to an act of war in the Clausewitz an sense, with the intent to create mass social panic'.

Challenges

Actions which take place in cyberspace or on the virtual battlefield may be difficult to identify and therefore to attribute with sufficient accuracy. Although their impact can certainly be felt in the physical realm and in normal life, these attacks take place surreptitiously. Was the attacker a foreign power or a small group of bored youths? Furthermore, the absence of immediate, visible harm and damage can mean that cyber-attacks are regarded as somewhat removed from reality, perhaps even as science fiction. In cyber warfare the boundaries are blurred between the military and the civilian, the physical and the virtual, and power can be exerted by states or non-state actors, or by proxy.

Hostile Actions Short of Warfare

Although some actions may appear aggressive and warlike, they may not necessarily be intended as acts

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

of war. In fact, to ensure a rational and proportionate response it can be far from useful to escalate an apparently hostile action to the status of warfare when it might more appropriately be countered at a lower level. This is not to say that hostile actions in cyberspace should not be taken seriously: far from it. But wherever possible distinctions should be drawn between the responses appropriate to different types and levels of cyber action. This should make it more likely that resources will be allocated most effectively and efficiently and it should be possible to reserve valuable political capital for the most serious and harmful of attacks. The first and most important distinction to be drawn is between those actors whose behavior in cyberspace can best be described as cyber warfare, and those who, while still constituting a security threat, operate at a separate and lesser level and require a different response. However, there are neither discrete, clearly defined 'camps' of users nor a 'simple hierarchy of threats.

Cyber actors are inherently difficult to categorize and defy rigid definitions, and their activities and the consequences of their activities can overlap considerably. If it is important to distinguish between warfare and non-warfare in cyberspace, then it follows that the distinction must be allowed to be mobile and flexible: a challenge for national strategy, perhaps. In other words, it is the action and its warlike properties that matter as much as the actor. That said, it seems reasonable to suppose that of the four types of threat domain put forward in the March 2009 Chatham House report, two seem most likely to generate acts of cyber warfare: state actors, and terrorist or extremist organizations. Hostile behavior in these domains will probably require an orchestrated, strategic and warlike response involving government and the security agencies and perhaps also the armed forces and industry.

However, the other two domains organized criminals and individual hackers principally attack the commercial sector and private individuals for financial gain or for malicious gratification. These threats should be met at the appropriate level societal, organizational or individual. This is not to say that criminals and lone hackers, or a group of nomadic hackers, could not launch an attack with warlike effects at some point in the future, but at present a largescale or warlike response to such actions seems disproptionate. The policy challenge, therefore, is to know what is cyber warfare and what is not, and to ensure that responses are proportionate not just to the hostile action, but also to the actor [7].

DISCUSSION

Having sought to distinguish between those hostile acts that can be described as warfare and those that cannot, we then find that warfare itself is a difficult and contentious concept. Richard Clarke argues that 'cyber war is a wholly new form of combat, the implications of which we do not yet fully understand'. Yet in many ways cyber warfare differs little from conventional or unconventional forms of warfare. Cyberspace has merely extended the battlefield and should be viewed as the fifth battlespace alongside the more traditional arenas of land, air, sea and space. It distorts our fledgling understanding of cyber warfare to argue that it is a conflict space in its own right. Simply put, cyber warfare is a new but not entirely separate component of a multifaceted conflict environment. It follows that cyber warfare should generally not be viewed as an independent or stand-alone occurrence. Few of the actions described above would deliver a decisive victory on their own and in any case, as Alex Michael observes: 'what remains unremarked in the popular narrative is a constant ongoing background level of cyber-attack as part of a holistic, coordinated program to achieve the political, economic and social aims of nation states'. Cyber-attacks provide force multiplier effects and are just one component of the broader strategic ways and means employed by a state or non-state group. As such, warlike challenges in cyberspace are more likely to occur in conjunction with other methods of coercion and confrontation [8]–[10].

CONCLUSION

Nevertheless, cyber warfare remains undeniably distinct from these other methods. Unlike diplomacy, military force and economic warfare, it challenges the traditionalist view of the state as the principal actor in the international system and the decisive influence on warfare. Although nation-states have far greater access to the capabilities, resources and budgets needed to carry out substantial and well-directed cyber-attacks, and are the most likely to employ cyber ways and means to achieve their ends and have already recognized its defensive and offensive potential, cyberspace has made it possible for non-state actors, commercial organizations and even individuals to acquire the means and motivation for warlike activity. Asymmetries in conflict are often exaggerated, with

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

the underdog often supposed to be more cunning and resourceful than he actually is, and more likely to succeed. Yet asymmetric warfare can be extremely potent, and prone to imitation. According to the recently appointed UK Chief of the Defense Staff, the lesson drawn by the opponents of the United States and the United Kingdom from operations in Iraq and Afghanistan is that for 'relatively little cost, unsophisticated opponents with very cheap weaponry' can pose a strategic threat. Much the same can be said for cyberspace. At comparatively low risk, significant damage and disruption can be inflicted on the intended target with little fear of reprisal. As a result, cyberspace gives disproportionate power to small and relatively insignificant actors.

REFERENCES

[1] M. J. Assante, "Implications of cyber in anti-access and area-denial counters," in *2016 IEEE International Conference on Cyber Conflict, CyCon U.S. 2016*, 2017. doi: 10.1109/CYCONUS.2016.7836611.

[2] M. R. O. Díaz and P. E. S. Rangel, "National challenges for cybersecurity on a global level: An analysis for colombia," *Rev. Crim.*, 2020.

[3] J. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke L. Tech. Rev.*, 2010.

[4] D. T. L. Tinker, G. McLaughlin, and M. Dumlao, "Risk Communication And Social Media: Tips and best practices for using new tools to communicate effectively," *Disaster Resour. Guid.*, 2015.

[5] K. Coleman, "The weaponry and strategies of digital conflict," in *5th European Conference on Information Management and Evaluation, ECIME 2011*, 2011.

[6] P. Giannetakis, L. Iannilli, and F. Caravelli, "Cyber Humint. A Behavioral Analysis Perspective," 2020.

[7] N. Manoharan, "India's Internal Security Situation: Threats and Responses," *India Q.*, 2013, doi: 10.1177/0974928413503748.

[8] E. Heffes, "The Oxford Handbook of the Use of Force in International Law," *J. Use Force Int. Law*, 2016, doi: 10.1080/20531702.2016.1221246.

[9] T. Saadawi and L. Jordan, *Cyber Infrastructure Protection*. 2011.

[10] N. P. Romashkina, "New technologies: Challenges to international security and stability," in *CEUR Workshop Proceedings*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Strategic Problem and Strategic Solution in Cyber Warfare

Ms. Archana Sasi
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-archanasasi@presidencyuniversity.in

ABSTRACT: ***Having examined cyber warfare according to a traditional blueprint for strategic analysis the 'action' of aggressive adversaries versus the 'reaction' of defending governments we attempt in this chapter to place our assessment of cyber warfare more firmly within the debate on national strategy and security policy. The first task is to be clear what cyber warfare is and why it matters strategically. We have shown that there is both continuity and discontinuity, tradition and novelty in cyber warfare. The first part of this chapter draws together these observations to establish the limits of our knowledge and understanding of cyber warfare as a strategic problem, and to identify where further analysis and reflection would be appropriate. To persist with our earlier maritime metaphor, in cyber warfare the challenge is to identify where navigators can safely use their skills and where there is a need for more work to chart unknown waters.***

KEYWORDS: ***Cyber Security, Cyber Threats, Computer Virus, Cyber Warfare, Internet.***

INTRODUCTION

The ability our nation has to create and maintain an ongoing process that may advance our national interest. In addition, it states that coping with complexity, ambiguity, and dynamic situations is what strategy is all about. It is not a strategy or document. In contemporary politics, it is important to make sure that the whole government recognizes and serves the national interest. The select committee also looked at how strategy and policy relate to one another, stating emphatically that "strategy is not policy, but is the means to effect it." The statement in their study that "strategy is what gives policy its ways and means, and [military] action its ends" was made by Paul Cornish. This point of view contends that strategy is best understood as making sense of both action (military or otherwise) and policy. The third iteration of the UK National Security Strategy, which was also released in October 2010, has a similar perspective of strategy: Like any other plan, a national security strategy must include goals, tactics, and resources [1]. It seems that the United States has a similar understanding of the issue: "US officials acknowledge they cannot resolve the cyber security issue by simply applying more human and technological resources." A thorough plan for cyber operations is also required, as well as new tactics, methods, and processes.

The 'Ends' of Cyber Warfare

Regarding the reasons why governments would choose to use cyberwarfare, when and under what circumstances, as well as the reasons they might decide not to, there is no general agreement and little conventional knowledge. There isn't a developed, well acknowledged legislative, regulatory, or normative framework for cyber warfare as a concept or as a collection of behaviours. This is not to suggest that cyberspace is unregulated or that there are no opinions on what may or may not happen there and how it may be used. The social networking site Facebook, for instance, has restrictions concerning which third-party apps may be launched on its site and how personal data may be used. Regulations and even normative limitations may be found at some levels and in specific sectors of the internet.

It even has a website dedicated to promoting peace called "Peace on Facebook," which aims to "play a part in promoting peace by building technology that helps people better understand each other." We can lessen global violence in the short and long runs by making it simple for individuals from different backgrounds to communicate with one another and exchange ideas. However, given the expanse of cyberspace, these isolated incidents hardly represent the consensus view of all internet users worldwide. Sadly, it's unlikely that "Peace on Facebook" will lead to the establishment of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

a worldwide framework for weapons control and non-proliferation online. Of course, this evaluation may alter. This research makes the case that these individual self-regulation attempts must be replaced by a worldwide initiative that is both ambitious in scope and binding in application [2].

As previously mentioned, it can be very difficult to determine the purpose or even the identity of a cyber-aggressor at the operational level, making it challenging to discuss cyber warfare in terms of a traditional strategic analysis as an action by a known party using specific resources to achieve specific goals. Any debate or reporting on cyberwarfare often brings up the "attribution problem": "Attribution is the key to understanding the motive of an attack and, consequently, being able to differentiate between a criminal act and warfare in cyberspace. It is crucial for coordinating national and international responses and determining national policy."

But attribution is not a straightforward issue. Since cyberwarfare, cyberterrorism, cybercrime, and cyberfiction may all employ similar "tactics, techniques, and procedures," it can be difficult to discern between various cybersecurity threats. Cyberspace good known as "plausible deniability," which is in abundant supply, can make it challenging to prove beyond a reasonable doubt that the government of a state may have been responsible for a cyberattack launched with private computing means from the territory of a second state on the electronic infrastructure of a third.

The identity and purpose of the attacker could not be known before the commencement or even the end of an assault without quick and precise attribution. A defending government will find it challenging to determine that its reaction is both precisely targeted and appropriate to the harm done without such attribution. It is seldom obvious who is targeting whom, as The Economist pointed out in a comment on the 2010 Stuxnet assault on Iranian nuclear facilities. It might be difficult to determine if a strike has been effective or even what has transpired. This seems to be how cyberwar looks. Learn to accept it.85 If this accurately describes the "attribution problem," it highlights a significant difference between cyberwarfare and conventional warfare. The prevalent assumption in the traditional strategic paradigm of state-based defiance against opponents, whether other nations or even terrorist organizations, was that the intention and in fact, the identity would be adequately exposed in the act itself [3].

Ways of Cyber Warfare

What may be anticipated from using cyberwarfare to accomplish strategic goals, and how far-reaching might those goals be as a result? Depending on the level of decisiveness that can be assigned to cyber warfare and where it falls on a spectrum of strategic tactics, the answers to these questions will vary. The first issue is that, on such a spectrum, cyberwarfare might be positioned in at least four different places. One theory, mentioned in Chapter 1, claims that cyber warfare is nothing less than a whole new and adequate explanation for war in the twenty-first century: "There have even been suggestions that future wars could be fought entirely in cyberspace, replacing conventional military operations."86 It is equally common to find references to the possibility of a "cyber Pearl Harbour" and "cybergeddon" in the reporting of cyberwarfare and in what passes for scholarly literature on the subject, as it is to find vehement attempts to dismiss such possibilities as scaremongering and worst-case analysis. Our study has led us to take a more circumspect approach to the possibility of cyberwar, but how can we, as well as the broader audience, be sure that we are correct and that others, like Michael Markulec, who claims that "the severity of the threat has been understated," are mistaken? The second idea is that cyberwarfare should be seen more as a separate branch of military operations to be positioned alongside land, sea, and air operations on the strategic spectrum: "Much like land, sea, and airpower, cyber-power is a weapon of war."88 When space operations and cyberwarfare are combined, we reach the notion of a "fifth battlespace."89 The argument would be that all five of the so-called "battlespaces" must be seen as necessary to the total, rather than that any one of the five might be significant on its own in military operations.

The third possibility is that this gives cyber warfare more importance than it actually does and that, rather than being given its position on the strategic spectrum, it should only be viewed as an auxiliary function or "force multiplier" for the current four battlespaces, similar to radio communications or target surveillance. The fourth and most straightforward alternative is to simply think about cyberwarfare in terms of the "weapons" it may provide to a broad range of users and the potential consequences such weapons may have on communities, governments, enterprises, and other entities. There may even be a fifth possibility, according to which cyberwarfare should not be categorized with other strategic tactics since it is

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

inherently non-strategic [4].

The possibilities listed above are all realistic. In terms of the difficulty for national policy, this must distinguish cyber warfare from other, more traditional concepts of warfare because it offers everything not because it promises anything completely new or noticeably different. Quantity, according to a quote attributed to Stalin has a quality all of its own. In other words, as a tactical approach, it demonstrates that offensive action is generally simpler, faster, and less expensive than defensive action. Cyber warfare may be the classic example of what is today referred to as asymmetric warfare a conflict in which one side may be strong but cunning and adaptable, while the other side is powerful but complacent and rigid.

The terrorist attacks that occurred in the United States in September 2001 are a powerful illustration of asymmetric warfare: the world's military superpower was assaulted by a tiny number of terrorists who used crude weapons and tactics to terrible effect. Similar, if not much bigger, possibilities are available in cyberspace. The United States has a defiance budget of around $700 billion each year. However, a cyber security researcher claims that it would only take two years and less than $50 million per year to plan a cyberattack that could paralyse the US. This operation 'may entail fewer than 600 individuals trying to infect systems,' the analyst said. The practice of asymmetric cyberwarfare must not belong to lone actors or small organizations.

To counterbalance the conventional military advantages enjoyed by an adversary, in this case the United States, a state can invest in cyberwarfare capabilities and attack a vitally important component of the adversary's defensive infrastructure, in this case the US military command-and-control organization [5]. It may be difficult to predict with great precision how asymmetric cyber warfare may affect both low- and high-level operations. Unlike a physical attack intended to sabotage or destroy a factory or transport node, for example, a cyberattack against a key location or facility typically uses information and communication networks to exploit and corrupt to achieve the desired effect indirectly. Neither the attacker nor the defence will likely be aware of the entire scope of the assault, the network's vulnerability, or if the attack will have an impact on other connected networks.

Therefore, it is feasible to imagine inadvertent asymmetric cyber warfare, where the outcome may be beyond the control and expectation of both the attacker and the defiance, in addition to both low-level and high-level asymmetric cyber warfare. Asymmetric cyber warfare is difficult to fight against, and it is also hard to see how governments could give up on the endeavor and accept total exposure to the kinds of attacks mentioned above. Imposing export and proliferation restrictions on important technology would be feasible, but considering that most of today's "cyber weaponry" takes the form of software, it might not be a good idea to place too much faith in this traditional solution. Instead, to balance the equation between attack and defiance and eliminate the asymmetric advantage, governments may decide to respond to the asymmetric security challenge in a similar manner to how they have in the past, for instance, when dealing with terrorists and insurgents. In other words, maybe there is a place for 'counter-hackers' hired by the government inside the intelligence community or for a 'Hacktivist Battalion' within the armed forces [6].

It's probable that these organizations already exist, hidden beneath the customary shroud of secrecy that envelops the signals and electronic intelligence industries. However, the level at which this capacity would be controlled much as how Special Forces are managed at the highest level of national command, despite their tactical maneuvering will be crucial if they are to be integrated into the mainstream of national policy. The assignment of these resources will be challenging since the success of a tactical skirmish in a crucial area of a crucial battlefield which is also crucial politically and strategically could determine the course of an entire campaign. How might a commander of an infantry unit, who is being pinned down by precise conventional artillery fire, order "cyber fires" from locations that may be thousands of miles distant in order to disable the enemy forces' weapon-aiming computers? Finally, a quick discussion of deterrence is necessary before moving on to the "ways" of cyberwarfare. As was previously said, strategy is the utilization of certain methods and tools to accomplish specific goals. However, a plan need not necessarily include taking action. Sun Tzu said that "to win 100 victories in 100 battles is not the acme of skill" around 2,500 years ago.

The pinnacle of expertise is to subjugate the opponent without engaging in combat. It is possible to use strategy to stop an opponent's action from succeeding, to threaten an adverse response that would deter the opponent from acting in the first place, or, ideally, to convince him to concede defeat. Deterrence has

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

always been a component of strategy and defiance in one form or another, whether it takes the form of denying the enemy victory by erecting powerful defenses or by threatening to punish the enemy with some type of vengeance. Deterrence, however, seems to be particularly difficult to implement in cyberwarfare. It will be challenging to determine what has to be denied and who or what should be punished with punitive reprisal due to the "attribution problem" noted earlier and the general opaqueness of cyberspace. The ability to penalize and/or deny must be conveyed to the opponent, who must be identified, in order for deterrence to be effective.

Means of Cyber Warfare

Of course, both individuals and organizations of people must participate in cyberwarfare. However, it is appropriate to think of the "means of cyber warfare" as primarily technological: the "hardware" of communications and information infrastructures and the "software" that powers them. This is not unexpected since there has always been a link of sorts between technology, the application of science and innovation, and strategy (the deployment of forces and resources to attain political aims). However, the technology of cyberwarfare poses a challenge to conventional wisdom on this relationship in at least three ways.

Many researchers and pundits believe that the ability of threats to adapt quickly is what makes cyberwarfare and cybersecurity in general so special. Even towards the conclusion of the George W. Bush administration, according to former CIA director Michael Hayden, "cyber was moving so fast that we were always in danger of building up precedent before we built up policy." The conventional, action/reaction cycle of strategic evolution may become obsolete before it has even begun due to the abrupt pace of change. It is as if a government operational analyst had been sent to study the effects of the flintlock musket in combat only to find out upon arrival that the Maxim gun had been developed instead [7].

The 'offensive dominance' mentioned above may likely to result from the speed at which invention occurs in cyberspace, which may in turn encourage a first attack. Therefore, according to traditional strategic analysis, the "ways" of cyberwarfare might lead to "crisis instability" and "arms race instability." In a crisis, the first of these forces governments to take action initially, usually sooner than would otherwise be required. Cyber capabilities may be seen under these extreme pressures in a similar manner as nuclear weapons were in the early days of thinking about nuclear deterrence, when the decision appeared to be clear-cut: "use them or lose them." On the other side, instability in the weapons race will foster a tit-for-tat increase in power: a virtual arms race. Governments would undoubtedly want to tap into sources of knowledge and innovation in order to respond to threat development more quickly given the extremely fast growth of cyber risks. In light of this, they could want to collaborate with businesses and academic institutions. But it will be crucial to remember one of the lessons from the nuclear age: innovation may, paradoxically, make the system as a whole less stable, even while it can solve individual risks.

The second distinguishing characteristic of cyber warfare strategic "means" is that normalcy is exploited by cyber technology in a covert, if not undetectable manner. The utilization of familiar land, sea, air, and space platforms has long been a tactic used by conventional military activities to take advantage of normalcy. What makes this technique unusual is that these channels have often been used in highly developed, specialized, and visible ways. The same principles of flying are used by passenger liners and war aircraft. The future aircraft carriers for the Royal Navy may have a displacement that is comparable to that of a Panamax container ship. And much like a big earth mover, a main battle tank will utilize its treads to navigate rocky terrain. There should never be any ambiguity as to what is military or even just confrontational and what is not in any of these situations. The same cannot be true of cyberspace technologies. There is some overlap since a cyber-aggressor and a nuclear submarine both have the ability to strike and vanish without leaving a trace. The main distinction is that non-state actors can afford more potent and covert cyber-weapons, but the cost of similar conventional weapons is beyond all but the most developed governments. Finally, cyber warfare has been democratized as a strategic "means," but in an odd and empty way. Technologies that were formerly thought to be highly specialized have spread to become broadly accessible and somewhat user-friendly [8].

DISCUSSION

Cyberspace has rapidly advanced into a technical norm on a worldwide scale. However, it seems that the values, concepts, and standards that ought to guide

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

human behavior particularly, and intriguingly, while a common is being built have not advanced at the same rate. This is not to imply that morals and values are completely absent from cyberspace; rather, examples like the Facebook instance from earlier or the Chinese "human flesh searches" that harness the strength of the masses to find and shun those who need to be punished for some infraction serve to highlight this point. But it's crucial to keep in mind that laws and standards have been atomized; they are now accessible as "apps" or free software that any computer user may customize and use (if they so want). If Clausewitz's theories are still valid, then there may be as many interpretations of them as there are users of cyber technology, we may argue [9], [10].

CONCLUSION

There are two aspects to the strategic response to cyberwarfare. First and first, the task must be to extend politics and policy into cyberspace in order to more strictly regulate and standardize cyber warfare. Politics, on the other hand, must accept and adapt to the problems of cyber warfare if it is to be normalized by politics. The second goal is to apply the intricacies of cyber warfare to politics while examining and updating many of the underlying presumptions that underpin the state-centric, government-led approach to warfare advocated by Clausewitz. In other words, the Clausewitz Ian framework of analysis must be modified by cyberwarfare, but it must also be transformed by cyberwarfare. There are three stages to this politicization process. The first step is to reject the prevalent viewpoint that cyberwarfare is seen as a disjointed collection of more or less scary tales, with each incidence needing an ad hoc reaction of some kind. In order to know how to effectively deal with it, cyber warfare has to be examined holistically and subjected to some analytical rigor.

REFERENCES

[1] A. Chevallier, “An Overview of Strategic Thinking in Complex Problem Solving,” in Strategic Thinking in Complex Problem Solving, 2016. doi: 10.1093/acprof:oso/9780190463908.003.0001.

[2] M. Bichler and J. K. Goeree, “Frontiers in spectrum auction design,” Int. J. Ind. Organ., 2017, doi: 10.1016/j.ijindorg.2016.05.006.

[3] M. Purbrick, “A REPORT OF THE 2019 HONG KONG PROTESTS,” Asian Aff. (Lond)., 2019, doi: 10.1080/03068374.2019.1672397.

[4] L. (Don) A. N. Dioko, “The problem of rapid tourism growth – an overview of the strategic question,” Worldwide Hospitality and Tourism Themes. 2017. doi: 10.1108/WHATT-02-2017-0005.

[5] A. Caris, C. Macharis, and G. K. Janssens, “Planning problems in intermodal freight transport: Accomplishments and prospects,” Transp. Plan. Technol., 2008, doi: 10.1080/03081060802086397.

[6] M. Marć, A. Bartosiewicz, J. Burzyńska, Z. Chmiel, and P. Januszewicz, “A nursing shortage – a prospect of global and local policies,” International Nursing Review. 2019. doi: 10.1111/inr.12473.

[7] A. Bris et al., “KNIGHTS, RAIDERS, AND TARGETS - THE IMPACT OF THE HOSTILE TAKEOVER - COFFEE,JC, LOWENSTEIN,L, ROSEACKERMAN,S,” J. Bank. Financ., 2021.

[8] C. Martínez-Costa, M. Mas-Machuca, E. Benedito, and A. Corominas, “A review of mathematical programming models for strategic capacity planning in manufacturing,” International Journal of Production Economics. 2014. doi: 10.1016/j.ijpe.2014.03.011.

[9] S. Zajac and S. Huber, “Objectives and methods in multi-objective routing problems: a survey and classification scheme,” European Journal of Operational Research. 2021. doi: 10.1016/j.ejor.2020.07.005.

[10] J. K. Brueckner, “Strategic interaction among governments: An overview of empirical studies,” Int. Reg. Sci. Rev., 2003, doi: 10.1177/0160017602250974.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of the Cyber Space

Mr. Pinnapalli Prasad
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-prasadps@presidencyuniversity.in

ABSTRACT: ***Modern life is now completely reliant on cyberspace, the enormous, linked universe of computer networks and virtual worlds. It has transcended geographical barriers, giving people access to previously unheard-of possibilities for discovery, sharing, and connection. The complex character of cyberspace is explored in this abstract, along with the technical foundations, sociological ramifications, and interactions between people and the digital environment. These papers try to shed light on the complex dynamics influencing our experiences in cyberspace by synthesizing various viewpoints from the domains of computer science, sociology, and psychology. This abstract aims to further our comprehension of the constantly changing cyberspace environment and its enormous influence on our lives by examining subjects including online identities, privacy issues, virtual communities, and cybersecurity.***

KEYWORDS: ***Artificial Intelligence, Big Data, Blockchain, Cloud Computing, Cryptocurrency, Cyber Attacks, Cybersecurity***

INTRODUCTION

One of the most significant innovations of the twenty-first century that has changed our lives is the internet. The way we communicate, play games, work, shop, make friends, watch films, order meals, pay bills, and greet pals on their birthdays and anniversaries has all been altered by the internet. Anything you can think of, we have an app for it. It has made our lives easier by enhancing their comfort. The days of having to wait in line for hours to pay our phone and power bills are long gone. We may now pay it instantly from our home or place of business. We no longer even need a computer to use the internet because of advancements in technology. We now have internet-enabled smartphones, palmtops, and other devices that allow us to stay in touch with our friends, family, and workplace around the clock. The internet has not only made our lives simpler, but it has also made many items more affordable for the middle class. Not so long ago, when making an ISD or even STD call, the pulse meter caught our attention. The calls cost a lot of money. Only urgent messages were sent via ISD and STD; all other normal communications were conducted using letters since they were so inexpensive. A one-hour video chat over the internet is now more affordable than the cost of sending a single page of text from Delhi to Bangalore via speed post or courier service, thanks to the internet's ability to do both talking and video conferencing for a very low price. Additionally, the way we utilize our regular equipment has altered as a result of the Internet. Popular TV series and films may be watched on television, but they can also be used to phone or video chat with friends through the internet. In addition to making calls, many use their phones to watch the newest films. No matter where we are, we can always stay in touch with everyone. Working parents may watch over their kids at home and assist them with their schoolwork. A businessman may easily monitor his employees, workplace, store, and other locations by clicking a button. It has improved our quality of life in several ways. Have you ever wondered how the internet was started? Let's talk about the short history of the internet and discover how it was created and how it developed to the point where we can no longer imagine life without It [1].

I'm not sure what the United States and Russia's Cold War contributed to the globe, but the internet is undoubtedly one of those very valuable innovations whose roots can be traced back to those turbulent times. On October 4, 1957, Russia launched SPUTNIK, the first satellite ever, into orbit. This was Russia's win in cyberspace, and in response, the United States Department of Defense's Advanced Research Projects Agency announced the beginning of ARPANET (Advanced Research Projects Agency Network) in the early 1960s. This was an experimental network that was built to keep computers linked to it in touch with one another even if a node failed to react

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

as a result of a bomb strike on it. The University of California, Los Angeles (UCLA) laboratory of Leonard Klein rock sent the first message across the packed switching network known as the ARPANET. You may be astonished to learn that "LO" was the first message ever transmitted across the internet. Actually, they were trying to transmit the word "LOGIN," but only the first two letters got to the second network node at Stanford Research Institute (SRI) before the network went down and prevented the next three letters from getting there. The message was delivered again when the problem was quickly repaired [2].

Creating protocols for communication via ARPANET, or the rules for communication, is the main responsibility of ARPANET. The invention of internetworking protocols, which allowed numerous independent networks to be connected to form a network of networks, was particularly influenced by the ARPANET. It led to the creation of the TCP/IP protocol suite, which outlines the guidelines for connecting to and interacting with the APRANET. Soon after, in 1986, the NSF (National Science Foundation) backbone was established, and the computer facilities of five US colleges were linked to create NSF net. The following universities took part:

i. **Princeton University:** John von Neumann National Supercomputer Center, Jv NC
ii. **Cornell University:** Cornell Theory Center, CTC
iii. **University of Illinois at Urbana-Champaign:** National Center for Supercomputing Applications, NCSA
iv. **Carnegie Mellon University:** Pittsburgh Supercomputer Center, PSC
v. **General Atomics:** San Diego Supercomputer Center, SDSC

By 1990, NFS net, the ARPA net's replacement, had gained popularity, and ARPANET had been shut down. Other universities and nations, such as the UK, built a number of similar networks. A packed switching network was suggested in 1965 by the National Physical Laboratory (NPL). The National Science Foundation (NSF) and the State of Michigan provided funding and assistance for the establishment of the MERIT network by the Michigan Educational Research Information Triad in 1966. In 1973, the CYCLADES packet switching network was created in France [3].

Now that there were several parallel systems operating under various protocols, scientists were searching for some kind of unifying standard to enable the networks to be joined. TCP/IP protocol suites were available by 1978, and ARPANET adopted the protocol in 1983. The merger of two sizable networks happened in 1981. The TCP/IP protocol suite was used by NFS to connect to the ARPANET and create the Computer Science Network (CSNET). Now, the network was not only well-liked by the scholarly community, but also by the general public. NFS initially provided 56 k bit/s of speed. In order to support the network's expansion, the state of Michigan, IBM, MCA, and the Merit Network expanded it to 1.5 Mbit/s in 1988.

As soon as the partners saw the value and power of the network, they became involved in its growth to reap its rewards. Many Internet Service Providers (ISPs) started to appear during the late 1980s, acting as the network's backbone. NFSNET was expanded and improved to 45Mbit/s by 1991. Many commercial ISPs offered backbone services and were well-liked by businesses. NFSNET was shut down in 1995 so that the network could be used for commerce, allowing the Internet to handle commercial traffic.

It is now linked to an increasing number of universities and research institutions worldwide. Now that this network was well-liked by the scientific community, the National Research and Education Network (NREN) was established in 1991, the same year that the World Wide Web was made public. The sole purpose of the internet at first was for file transfers. Tim Berners-Lee invented www, which had a significant impact on how the internet was utilized. He is responsible for the internet as we know it today. Now, any information that is accessible on the internet may be retrieved through this informational web. To surf the internet, a program called a browser was created. It was created in 1992 by scientists at the University of Illinois and given the name Mosaic. With the help of this browser, you may use the internet the same way we do now.

DNS

We seldom enter IP addresses like 104.28.2.92 while browsing websites on the internet; instead, we use names like www.uou.ac.in. However, even if we enter http:104.28.2.92 in the URL, we will still arrive to the same page. The truth is that humans find it far easier to use and recall names than numbers. Furthermore, some of the websites have various IP addresses, and these IP addresses fluctuate over time. Additionally, since IP addresses are used for routing internet-based data packets, only IP addresses may be used for data transmission over the internet. Domain Name System (DNS) is a service that handles this translation task in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

order to make things simpler and save us from having to memorise these altering IP address numbers. Every time you write an address like http://www.uou.ac.in, a background operation known as DNS name resolution takes place. The computer maintains a local database in the DNS cache and keeps track of recently visited websites. If the DNS cache on your local computer does not have the IP address of the website you have accessed, your Internet Service Provider's (ISP) DNS server is likely to contain it. The cache of recently accessed sites is likewise kept on these ISP DNS servers. The DNS server of the ISP forwards the request to the root name servers just in case the information is not available there as well. To other DNS servers and clients on the Internet, the root name servers provide the root zone file. The authoritative servers for the DNS top-level domains (TLDs) are listed in the root zone file. Right now, there are 13 Root name servers. As follows [4]:

- **a)** VeriSign Global Registry Services
- **b)** University of Southern California - Information Sciences Institute
- **c)** Cogent Communications
- **d)** University of Maryland
- **e)** NASA Ames Research Center
- **f)** Internet Systems Consortium, Inc.
- **g)** U.S. DOD Network Information Center
- **h)** U.S. Army Research Lab
- **i)** Auto nomica/NORDU net
- **j)** VeriSign Global Registry Services
- **k)** RIPE NCC
- **l)** ICANN
- **m)** WIDE Project

By reading the last portion of the URL first, these root name servers send the query to the proper Top-Level Domain (TLD) name servers. The URL in our sample was http://www.uou.ac.in. The last character is.in. The following are a few instances of TLD name servers: .com, .biz, .org, .us, .in, and so on. By acting as a switchboard, these TLD name servers route the request to the relevant authoritative name servers that are maintained by each domain. These reliable name servers keep track of DNS records as well as other helpful data. TLD name servers, name servers, and the DNS server of the ISP all provide this address record back to the asking host computer. To avoid having to repeat this procedure every time the same request is made, these intermediate servers save a record of this IP address in their DNS cache. If the same URL is asked once again, the local host computer's DNS cache will return the URL's IP address.

DISCUSSION

Internet Infrastructure

The Internet is a network of networks, as its name implies. It is made up of a number of small, medium, and big networks. This makes one thing very clear: The internet is one of the best instances of successful collaboration because no one person owns it. Now, you must be perplexed as to how such a sizable network that is dispersed throughout countries can function flawlessly. Yes, it is true that we need a worldwide organization to set the rules, regulations, and protocols for joining and using this network in order to monitor such a vast network. In order to address these challenges, a global organization called "The Internet Society" was established in 1992 [5].

Let's talk about how the internet works today. How your friend's computer, which is situated in a different nation or continent, interprets the email you sent them. Your computer is a standalone system while you are using your laptop or desktop at home and not connected to the internet. However, if you call into your Internet Service Provider (ISP) using your modem to access the internet, you join the network. The ISP serves as a conduit between the user and the internet backbone, which is where all data travels. Network Access Points (NAP) are the points where the ISP connects to the internet backbone. Large telecommunications firms in diverse locations offer these NAPs. By constructing and maintaining a sizable backbone infrastructure to transport data from NAP to NAP, these huge telecommunications corporations link the nations and continents. ISPs are in charge of constructing and managing local networks and are linked to this backbone at NAP. Therefore, when you connect to the internet via a modem, you first join the local ISP, which then uses NAP to connect to the internet's backbone. The data is transferred to the target NAP, which is home to your friend's network's ISP, through this backbone for routing. The data is sent to your friend's computer as soon as he calls his modem to access the internet.

World Wide Web

The terms "internet" and "world wide web," or simply "the web," are sometimes used interchangeably. However, the internet offers many more services in addition to the web. E-mail, Usenet, chat services, FTP, and other well-known internet services are available in addition to the web. The web uses the HTTP protocol to interact across the internet and to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

share information. British physicist Tim Berners-Lee created the web at CERN in 1989. It comprises of all publicly accessible websites and any hardware used to view online information. The World Wide Web is a paradigm for exchanging information that was created for online information exchange. On the internet, there are many public websites, which are just collections of web pages. These websites are filled with information in the form of text, videos, audio, and images. A program called a web browser is used to visit these online sites. Internet Explorer, Chrome, Safari, Firefox, and other well-known browsers are a few examples. This was a brief introduction to the internet and its operation. Let's now talk about cybercrime.

Introduction to Cyber Crime

Around the 1960s, only a small number of scientists, researchers, and those working in the defense had access to the internet. Expectedly, the Internet user base has changed. At first, computer crime was limited to physically harming computers and associated equipment. Around the 1980s, the focus shifted from physically harming computers to intentionally causing them to malfunction using malicious software known as viruses. Because internet was only integrated into defense systems, major multinational corporations, and research groups up until that point, the influence was not as ubiquitous. When the internet was first made available to the general public in 1996, it rapidly gained popularity among the populace and they gradually became reliant on it to the point where it altered their way of life. The user doesn't have to worry about how the internet works since the GUIs were developed so beautifully. Without worrying about where the data is stored, how it is sent over the internet, whether it can be accessed by someone else who is connected to the internet, or whether the data packet sent over the internet can be snooped and tempered, they simply need to click a few times on the hyperlinks or type the desired information at the desired location. Financial crime has become the main objective of computer crime, instead than just endangering the computer or erasing or modifying data for one's own gain. The frequency of these cyberattacks is rapidly rising. Up until 2013, 800 million people were impacted by cyberattacks, which occurred every second on around 25 computers. Between 2011 and 2013, CERT-India revealed that 308371 Indian websites have been compromised. Additionally, it is predicted that cybercrime results in annual losses of around $160 million. Given that the majority of instances are never recorded, this number is very cautious [6].

India has an estimated 100 million internet users as of June 2011, and the number is rapidly increasing, according to the 2013–14 report of the standing committee on Information Technology to the 15th Lok Sabha from the ministry of communication and information technology. There are now around 134 major Internet service providers (ISPs) operating 22 million broadband connections in India. Cybercrime is a word used to describe illegal conduct in which computers or computing devices, such as stand-alone or networked smartphones, tablets, Personal Digital Assistants (PDAs), are utilized as a tool or/and target of criminal action. People with destructive and criminal mindsets often conduct it either out of retaliation, money, or adventure.

Classification of Cyber Crimes

The organization that is the target of the cyberattack may have internal or foreign cybercriminals. This fact allows for the classification of cybercrime into two categories:

i. **Insider Attack:** An insider attack is when a user with authorized system access attacks a network or computer system. It is often carried out by angry or unsatisfied internal workers or contractors. The insider attack's motivation might be retaliation or greed. An insider may carry out a cyberattack relatively easily since he is well-aware of the security system's flaws and rules, procedures, and IT architecture. Additionally, the hacker has access to the network. Because of this, it is quite simple for an insider attacker to steal important data, bring down the network, etc. The majority of the time, an insider attack occurs when an employee is let go or given a new function inside an organization that is not reflected in the IT rules. For the attacker, this creates a window of verifiability. Planning and implementing an internal intrusion detection system (IDS) in the company might stop the insider assault.

ii. **External Attack:** This kind of attack occurs when the assailant is either employed by an inside or external party to the organization. The organization

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

that is the target of a cyberattack not only suffers financial loss but also reputational damage. Since the attacker is not a member of the organization, they often scan and acquire data. An experiment network/security administrator regularly monitors the logs produced by the firewalls since these logs may be used to identify external threats. Additionally, intrusion detection systems are set up to monitor outside threats.

Depending on the sophistication of the attacker, cyberattacks may also be divided into organized and unstructured assaults. Although some writers have categorized these assaults as an example of external attacks, there have been instances in which an inside employee has carried out an organized attack. This occurs when a rival business wants to know an organization's future strategy on certain issues. The attacker may carefully hire himself inside the firm to obtain access to the necessary data[7].

a) **Unstructured Attacks:** These types of cyberattacks are often carried out by armatures without any clear goals in mind. Typically, these armatures attempt to test a tool that is easily accessible online on the network of an unrelated business.
b) **Structure Attack:** These assaults are carried out by highly competent and experienced individuals, and their intentions are crystal obvious to them. As seen in Figure 1, they have access to sophisticated tools and technologies that allow them to penetrate other networks undetected by their intrusion detection systems (IDSs). These attackers also possess the know-how to create new tools or change those that already exist to serve their objectives. These kinds of assaults are often carried out by professional criminals, nations against other competitor nations, politicians to harm the reputation of the opponent individual or nation, terrorists, competing businesses, etc.

Cybercrime has shown to be a low-risk, low-investment industry with enormous profits. These organized crimes are carried out in a very organized manner nowadays. There is a flawless hierarchical organizational structure, similar to that of formal organizations, and some of them have advanced to a level in technology on par with that of industrialized nations. They prey on huge financial institutions, nuclear power plants, and defense sites. They also engage in internet drug trade.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

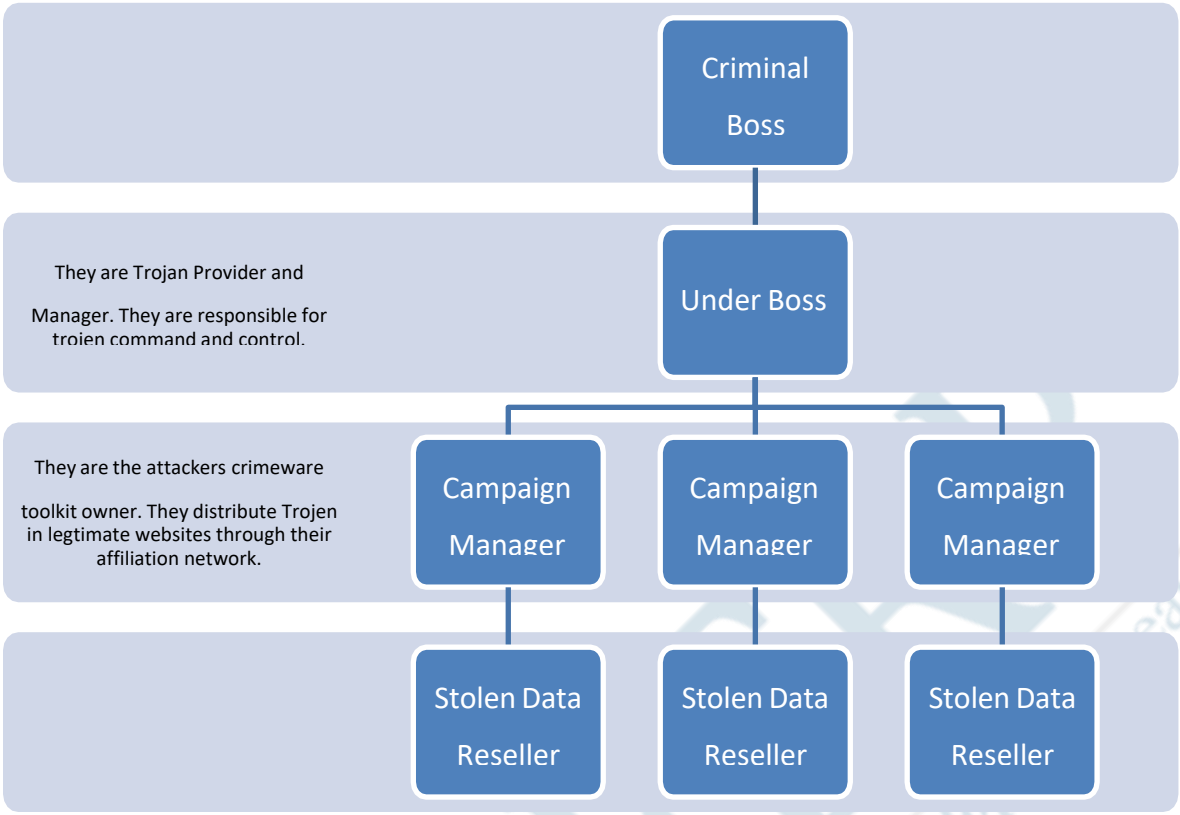

Figure 1: Illustrated the Hierarchical Organizational Structure.

Each person's position in the hierarchy changes throughout time and is determined by opportunities. If a hacker who has stolen private information from a company may utilize it to financially benefit himself from the company. If the hacker has the necessary technical know-how, he will do it himself; alternatively, he may locate a buyer with the necessary technical know-how who is interested in the data.

Some online criminals provide on-demand services. These cybercriminals may be contacted by an individual, an organization, or a nation to hack a target company to get access to private information or to launch a large-scale denial-of-service assault on a rival company. Hackers create malware, viruses, and other malicious software to meet client demands. A cyber-attack on a company may result in not only financial loss but also harm to the company's image and unquestionably benefits the rival company [7].

Reasons for Commission of Cyber Crimes

Several factors contribute to the expansion of cybercrime. The following are some salient reasons:

a) Money: The desire to earn fast, easy money drives people to conduct cybercrime.

b) Revenge: Some individuals attempt to exact vengeance on another person, organization, community, caste, or religion by damaging their reputation or causing them to suffer material or bodily harm. This fits the definition of cyberterrorism.

c) Fun: Amateurs commit cybercrimes. They just want to experiment with the newest tool they have come upon.

d) Recognition: If someone hacks into a highly guarded network, such as a defense site or network, it is seen as prying.

e) Anonymity: Often, the ability to stay anonymous in a cyberspace environment encourages someone to conduct a cybercrime since it is much simpler to do so than in the actual world. In the virtual environment as opposed to the physical one, it is far simpler to get away with illegal activities. There is a pervasive feeling of anonymity that might tempt normally moral people to compromise

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

their moral principles in the name of self-interest.

F. Cyber Espionage: On occasion, the government engages in cyber trespassing to monitor another individual, network, or nation. Political, economic, or societal factors might be to blame.

Malware and Its Type

Malware short for "Malicious Software" is created to access or be installed on a computer without the user's knowledge or permission. For the advantage of a third party, they carry out undesired actions on the host computer. A wide variety of malware exist that may significantly impair the operation of the host PC. Malware comes in a wide variety, from simple programs meant to irritate or divert the user to sophisticated programs that steal vital information from the host computer and transfer it to distant servers. Malware comes in a variety of forms and is widely available online. Popular examples include:

a) Adware

This particular kind of malware is employed to compel users to see advertisements. They either reroute the page to an advertising page or trigger the pop-up of another page that advertises a certain commodity or occasion. The businesses whose goods are promoted financially support this adware.

b) Spyware

It is a particular kind of program that may be installed on the target computer with or without the user's consent and is designed to steal sensitive data from the system. Most of the time, it collects user surfing data and sends it to a distant server without the user's awareness. They are often downloaded into the host computer when freeware, or free application programs, are being downloaded from the internet. Spywares come in many different varieties; they may monitor the host computer's cookies, operate as key loggers to steal important data like banking passwords, etc.

c) Browser hijacking software

Along with the free software distributed online, there is some malicious software that is downloaded and installed on the host machine without the user's awareness. This malware alters browser preferences and reroutes connections to unintended websites [8].

d) Virus

A virus is malicious software designed to harm the host computer by removing or adding files, taking up memory space by copying the code, reducing computer speed, formatting the host system, etc. It may be disseminated by email attachments, flash drives, digital photos, electronic greetings, audio or video clips, etc. A virus could be present on a computer, but it requires human interaction to function. A virus cannot infect the host PC until and unless the executable file (.exe) is run.

e) Worms

They belong to a group of viruses that can reproduce. Because they do not need human involvement to move over the network and propagate from the infected system to the whole network, they differ from viruses in that respect. Worms may spread through email, networks, or the operating system's vulnerabilities. The network becomes choked as a result of the worm's network-wide replication and expansion, which use up all available space and bandwidth.

f) Trojan Horse

Trojan horses are pieces of malicious software that trick the host computer into accepting them as legitimate applications. The user opens a link or downloads a file that seems to be from a reliable source and is said to be beneficial. It alters the data and causes harm to the host computer, but it also introduces a backdoor that allows a remote computer to take control of the host machine. It may join a botnet, or "robot network," which is a network of computers with malicious software installed on them and under the direction of a master computer. Zombies are the machines on this network that have malicious programs installed on them. Trojans don't propagate or infect the other machines in the network.

DISCUSSION

The way we interact, acquire information, and travel across the globe has been completely transformed by cyberspace, the digital frontier made up of linked computer networks and virtual worlds. It now plays a crucial role in how we engage with one another, how we behave, and how it presents us with both chances and difficulties. Online identities and the ever-fuzzier boundaries between our virtual and actual personas are a hot topics of conversation in the cyberspace world. Questions of authenticity, trust, and responsibility have arisen in online encounters as a result of our capacity to construct several identities, participate in selective self-presentation, and explore new parts of our personality. Furthermore, the creation of virtual communities in cyberspace has facilitated cross-border communication and cooperation among people with similar interests and passions. By fostering new

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

kinds of social interaction, these communities have made it possible for people to share ideas, develop support systems, and take action as a group. Thoughts concerning echo chambers, false information, and the fragmentation of public discourse are also brought up by the growth of online groups. The war against cyber-attacks, hacking attempts, and the security of sensitive data is also continuing as a result of the internet being a playground for bad actors. Cybersecurity is now of utmost significance, and strong defenses are required to protect our digital infrastructure. Cyberspace is also rife with privacy issues, including discussions about data collecting, monitoring, and how to strike a balance between individual privacy and state security. The ethical and legal ramifications that the evolving online environment brings about also continue to develop. It takes multidisciplinary cooperation among specialists in technology, sociology, psychology, law, and policy-making to address these complicated difficulties. A continuing conversation about cyberspace investigates the revolutionary potential of digital connectedness while juggling the delicate line between personal agency and social well-being [9], [10].

CONCLUSION

With its extensive networks, virtual worlds, and digital possibilities, cyberspace has integrated itself into our linked reality. It has changed how we interact with one another, exchange information, and communicate. The debate over cyberspace sheds light on the nuanced aspects and complexity of this digital frontier. The benefits and difficulties given by cyberspace are linked as we negotiate the spheres of online identities, virtual communities, cybersecurity, and privacy. While technology provides fresh opportunities for creativity, teamwork, and global communication, it also carries dangers like cyberattacks, false information, and privacy loss. It is imperative to address these issues going ahead by encouraging responsible digital citizenship, advocating for strong cybersecurity measures, and creating laws that strike a balance between individual liberties and societal well-being. We can jointly create a digital future that promotes creativity, diversity, and trust by embracing the revolutionary potential of cyberspace while being aware of its drawbacks. Continued discussion and multidisciplinary cooperation will be essential in ensuring that cyberspace remains a potent force for good change in this dynamic and ever-evolving environment.

REFERENCES

[1] N. T. Le and D. B. Hoang, “Can maturity models support cyber security?,” 2017. doi: 10.1109/PCCC.2016.7820663.

[2] M. M. Neag, “Inclusion of the Cyber Space in the Operational Environment of the Military Actions - A New Paradigm in the Military Thinking,” Int. Conf. KNOWLEDGE-BASED Organ., 2020, doi: 10.2478/kbo-2020-0013.

[3] I. Hermawan, I. Inayah, S. Sartono, S. Suharnomo, and I. R. Aulia, “Konsep Active-Participants-Cyber-Learning Dalam Mendongkrak Peran Orientasi Kewirausahaan Terhadap Kinerja : Sebuah Perspektif Orgnaisasi Pembelajar,” Epigram, 2020, doi: 10.32722/epi.v17i2.3461.

[4] C. Droege, “Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians,” Int. Rev. Red Cross, 2013, doi: 10.1017/S1816383113000246.

[5] M. T. Whitty and A. N. Carr, “Cyberspace as potential space: Considering the web as a playground to cyber-flirt,” Human Relations. 2003. doi: 10.1177/00187267030567005.

[6] P. van Gelder et al., “Safe-by-design in engineering: An overview and comparative analysis of engineering disciplines,” Int. J. Environ. Res. Public Health, 2021, doi: 10.3390/ijerph18126329.

[7] N. Malysheva and A. Hurova, “Legal Framework of the Space Activity Cybersecurity in the USA: Experience for Ukraine,” Law Rev. Kyiv Univ. Law, 2020, doi: 10.36695/2219-5521.3.2020.59.

[8] M. T. Whitty and A. N. Carr, “Cyberspace as potential space : cyber-flirt,” Hum. Relations, 2003.

[9] L. E. Motorina and V. M. Sytnik, “Existential, instrumental and cyber spaces as ontological modi of human being,” Nov. Prisut., 2020, doi: 10.31192/np.18.3.4.

[10] M. Rusu, “Content analysis of new means of communication in contemporary democratic states,” Cent. East. Eur. eDem eGov Days, 2018, doi: 10.24989/ocg.v325.21.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of the Cyber Crime

Ms. Yeluguddad Akshatha
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-akshathay@presidencyuniversity.in

ABSTRACT: ***In the digital era, cybercrime has become a widespread issue, offering significant problems to people, organizations, and society at large. This abstract examines the many facets of cybercrime, which includes a range of illegal behaviors carried out through computer networks and the internet. It draws attention to the development of cyber threats, such as hacking, identity theft, fraud, virus transmission, and the ever-evolving methods used by cybercriminals. Additionally, it examines the negative effects of cybercrime, which range from monetary losses and reputational harm to the invasion of personal privacy and threats to national security. To successfully battle and mitigate the constantly changing threat environment of cybercrime, the abstract emphasizes the critical relevance of cybersecurity measures, coordinated efforts amongst stakeholders, and the establishment of strong legislative frameworks.***

KEYWORDS: Cybersecurity, Data breach, Hacking, Identity Theft, Malware, Ransomware

INTRODUCTION

Cybercrime has emerged as a potent enemy in the quickly developing digital age, transcending national borders and conventional ideas of criminal behavior. Because of the pervasiveness of technology and the interconnectedness of computer networks, criminal activity has flourished, making cybersecurity a top priority for everyone from people to businesses to governments. The term "cybercrime" refers to a broad variety of illegal behaviors committed using computers and the internet to conceal their identities and exploit security flaws. Cybercriminals use constantly developing methods to penetrate, breach, and exploit digital ecosystems for monetary gain or to destroy crucial infrastructures, from hacking and identity theft to fraud and virus dissemination. Cybercriminals use sophisticated tools, tactics, and plans to maximize their illegal earnings while avoiding discovery, creating a constantly evolving terrain for cybercrime. The reasons why people engage in cybercrime might be anything from financial incentives to political action, espionage, or even just the excitement of finding weaknesses. Cybercrime may have serious repercussions that can damage people, organizations, governments, and even national security as technology develops and society grows more dependent on digital infrastructure [1].

The effects of cybercrime are extensive and diverse. Businesses may suffer massive financial losses as a result of fraud and theft, losing billions of dollars annually. People are in danger of identity theft, which may compromise their financial and personal information and have catastrophic effects on their life. Governments are also not immune from cyberattacks, which may target vital infrastructures, interfere with public services, or compromise highly sensitive data related to national security. Cybercrime also has the potential to undermine public confidence in online systems and impede the expansion of the digital economy. Cybercrime concerns demand a comprehensive and cooperative strategy to be effectively addressed. To build effective defense mechanisms, raise cybersecurity awareness, and create legal frameworks to punish cybercriminals, governments, law enforcement agencies, cybersecurity specialists, corporations, and citizens must collaborate. Additionally, it is essential to spend on research and development to remain ahead of the continuously changing strategies and equipment used by cybercriminals. In the digital era, cybercrime has evolved as a sophisticated and constantly changing menace. The urgent need for a coordinated and aggressive response is made clear by its potential to destabilize economies, violate individual privacy, and jeopardize security. We may work to create a safer digital environment that protects the interests of people, organizations, and society at large by promoting international collaboration, enhancing cybersecurity measures, and increasing public awareness [2]. Several forms of cybercrimes include:

a) Cyber Stalking

It is a kind of stalking, harassment, or threat via the internet or a computer. This is often done to slander a person using the Internet as a medium since it provides

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

anonymity, such as via email, social networks, instant chat, online posting, etc. False allegations, threats, sexual exploitation of children, surveillance, etc. are examples of the behavior.

b) Child Pornography

It is illegal to have a picture or film of a juvenile (under 18) engaging in sexual activity.

c) Forgery and Counterfeiting

Software piracy is the unlawful reproduction and distribution of the software for commercial or personal use. It falls within the category of IPR-related criminality. Songs, films, and other types of downloads are among the various offences that fall under IPR infringement.

d) Software Piracy and Crime related to IPRs

In order to promote political or social goals, it is described as the use of computer resources to frighten or compel the government, the general public, or any group within it.

e) Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives [3], [4].

f) Phishing

Through the use of email and the appearance of a reliable organization, personal and sensitive information about a person may be obtained. Phishing is used to steal identities, and personal data like usernames, passwords, and credit card numbers may be used to defraud users of their money. Vishing (voice phishing) is the term for identity theft carried out over the phone. Smishing is another kind of phishing when clients are tricked through SMS [5].

g) Computer Vandalism

Physical force or malicious programming is used to physically damage computer resources.

h) Computer Hacking

It involves altering computer hardware and software to achieve a purpose other than that for which they were originally designed. Hacking a computer system may be done for a variety of purposes, from testing one's technical prowess to securing, altering, or erasing data for social, economic, or political objectives. To uncover and address security flaws, corporations are now actively recruiting hackers or those who engage in the deliberate hacking of systems. These categories of hackers include:

i. **White Hat:** White hat hackers are those that hack a system to identify its security flaws and inform the organizations concerned so that preventative measures may be implemented to safeguard it from outside hackers. White hat hackers may be salaried employees of an organization hired to uncover security loopholes, or they may be independent contractors looking to establish their expertise in this area. They are often referred to as ethical hackers.

ii. **Black Hat:** In contrast to white hat hackers, black hat hackers intentionally damage the system. They could attempt to hack the system for social, political, or financial motivations. They discover the system's security flaws, save the data for themselves, and make use of it for their own or their organization's gain until the organization whose system has been hacked learns about it and installs security fixes. They are often referred to as crackers.

iii. **Grey Hat:** These hackers identify security flaws on a website, notify the site administrators, and offer to remedy the flaw for a consulting fee.

iv. **Blue hat:** A blue hat hacker is an independent computer security consultant that tests a system for bugs before it is released to find vulnerabilities that can be patched [6].

i) Creating and Distributing Viruses over the Internet

An organization may experience a loss of revenue and money due to the propagation of a virus. The loss comprises the cost of fixing the system, the cost of lost revenue due to downtime, and the cost of missed opportunities. If the hacker is discovered, the organization has the right to sue for an amount greater than or equal to the damage it suffered.

j) Spamming

Spamming is the practice of sending mass, unsolicited commercial messages online. If an email satisfies the following requirements, it may be considered spam

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

[7].

i. **Mass mailing:** The email is sent to a large number of recipients rather than a single one.
ii. **Anonymity:** The person's true identity is unknown.
iii. **Unsolicited:** The receiver has neither requested nor expected the email.

These spams not only annoy the receivers and clog up the network, but they also waste time and take up precious inbox memory.

k) Cross-Site Scripting

It is a practice to introduce a malicious client-side script into a reliable website. The moment the malicious script is run by the browser, it has access to cookies and other sensitive data and sends it to distant servers. Now, this knowledge may be used to get monetary gain or direct physical access to a system for one's profit.

l) Online Auction Fraud

Several reliable websites provide online bidding on the internet. Some cybercriminals use the popularity of these websites to their advantage, luring buyers into online auction fraud schemes that often result in either overpaying for the goods or never receiving it after making the purchase.

m) Cyber Squatting

It is the act of holding onto trademark domain names to later sell them to the organization holding the trademark at a greater price.

n) Logic Bombs

These are pieces of malicious software that have been injected. A certain circumstance sets off wicked behavior. If the circumstances persist, harmful activity starts, and depending on the action specified in the malicious code, they either destroy the data stored in the system or render it useless.

o) Web Jacking

A hacker gains access to an organization's website and either modifies it for political, commercial, or social purposes or bans it. Recent instances of web jacking include Pakistani hackers who took control of educational institutions' websites and showed an animation with Pakistani flags on the homepage. Another example is the 2014 Indian Independence Day celebration when Indian hackers compromised the Pakistani Railways website and showed the Indian flag on the homepage for many hours.

p) Internet Time Thefts

Internet time theft occurs when someone hacks their ISP's account and password and uses it to browse the internet at his expense.

q) Denial of Service Attack

It is a cyberattack in which the network is overburdened and often collapses as a result of an overload of pointless traffic that blocks real network communication.

r) Salami Attack

It's an assault that develops gradually and culminates in a significant attack. The changes are so minute that nobody notices them. Gaining access to a person's online banking and withdrawing money in such a modest quantity that the owner is unaware of it is an example of a salami attack. The banking website often has a default trigger set so that withdrawals below, say, Rs. 1000 are not notified to the account owner. A total withdrawal of a considerable amount will result from making many withdrawals of Rs. 1000 over time [8], [9].

s) Data Diddling

The data is altered before entering the computer system in this practice. After the data execution is complete, the original data is often kept. For instance, DA or the person's basic wage may be altered in the payroll information of an individual for payment calculation purposes. The total salary is substituted in the report by his real pay when the salary has been computed and paid to his account.

t) Email Spoofing

It is a method of altering an email's header information so that its source is hidden and it looks to a recipient that the email came from a different source than the source.

DISCUSSION

In today's digital world, cybercrime has grown to be a growing threat. With the quick development of technology, thieves have discovered fresh methods to take advantage of weaknesses and prey on gullible people, businesses, and even whole countries. Cybercrime has far-reaching effects, including financial losses, harm to one's image, and even dangers to national security. Cybercriminals use a variety of tactics, such as hacking, data breaches, phishing schemes, and identity theft, to get

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

unauthorized access to sensitive information and use it for their advantage. Furthermore, the prevalence of ransomware assaults has shown its capability to shut down whole networks and demand astronomical ransoms. The issue of cybercrime is a growing concern as society depends increasingly on online connectivity. To reduce the threats posed by cybercrime, it is essential for people, organizations, and governments to maintain vigilance, regularly upgrade security protocols, and spread cybersecurity knowledge. Fighting this constantly changing danger requires cooperation between a variety of parties, including law enforcement organizations, cybersecurity professionals, and technology businesses. We can only successfully combat cybercrime and provide a safer digital environment for everyone via teamwork and aggressive actions [10].

CONCLUSION

In summary, cybercrime presents a big threat in our society that is becoming more linked. The pervasiveness of digital technology has given thieves new ways to take advantage of and hurt people, businesses, and whole societies. Cybercrime has serious repercussions, including financial loss, the compromise of private information, and a risk to national security. Prioritizing cybersecurity measures, being attentive, and fostering an awareness culture are essential for people, organizations, and governments to confront this always-changing danger. To keep one step ahead of hackers, collaboration between stakeholders and ongoing technical breakthroughs are crucial. We may strive towards a safer digital environment where the dangers of cybercrime are reduced by investing in strong security systems, encouraging education and training, and enforcing stringent regulatory frameworks. To ensure that technology continues to enhance and improve our lives without compromising our security and privacy, it is our common obligation to defend both ourselves and our digital infrastructure.

REFERENCES

[1] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” Comput. Secur., 2021, doi: 10.1016/j.cose.2021.102248.

[2] M. M. L. Prasanthi, “Cyber Crime: Prevention & Detection,” IJARCCE, 2015, doi: 10.17148/ijarcce.2015.4311.

[3] T. Ambika and K. Senthilvel, “Cyber Crimes against the State: A Study on Cyber Terrorism in India,” Webology, 2020, doi: 10.14704/WEB/V17I2/WEB17016.

[4] S. Furnell and S. Dowling, “Cyber crime: a portrait of the landscape,” Journal of Criminological Research, Policy and Practice. 2019. doi: 10.1108/JCRPP-07-2018-0021.

[5] L. C. Bande, “Legislating against cyber crime in Southern African development community: Balancing international standards with country-specific specificities,” Int. J. Cyber Criminol., 2018, doi: 10.5281/zenodo.1467632.

[6] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, “A survey of cyber crimes,” Security and Communication Networks. 2012. doi: 10.1002/sec.331.

[7] M. R. Habibi and I. Liviani, “Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia,” Al-Qanun J. Pemikir. dan Pembaharuan Huk. Islam, 2020.

[8] C. Whelan and D. Harkin, “Civilianising specialist units: Reflections on the policing of cyber-crime,” Criminol. Crim. Justice, 2021, doi: 10.1177/1748895819874866.

[9] H. Djanggih and N. Qamar, “Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime),” Pandecta Res. Law J., 2018, doi: 10.15294/pandecta.v13i1.14020.

[10] M. Lagazio, N. Sherif, and M. Cushman, “A multi-level approach to understanding the impact of cyber crime on the financial sector,” Comput. Secur., 2014, doi: 10.1016/j.cose.2014.05.006.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of the Cyber Security Techniques

Ms. Kunjali yashaswini
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-yashaswini@presidencyuniversity.in

ABSTRACT: ***Due to the continuously changing nature of digital dangers and our increasing reliance on technology, the area of cyber security has grown more and more important. This essay examines several forms of cyber security and the role they play in protecting networks and information systems from harmful activity. With a focus on their functions in preventing unauthorized access, identifying and mitigating assaults, and maintaining data confidentiality and integrity, it offers an overview of essential methods such as encryption, authentication, access control, and intrusion detection. Furthermore, cutting-edge approaches like machine learning, artificial intelligence, and blockchain are investigated to highlight their potential to strengthen cybersecurity defenses. The report stresses the significance of implementing a multi-layered and proactive strategy to cyber security, integrating technological solutions, human skills, and strong policies to successfully manage the constantly changing cyber dangers of the digital era.***

KEYWORDS: Cybersecurity, Information Security, Network Security, Data Protection, Encryption Algorithms, Access Control

INTRODUCTION

Cybersecurity is crucial in the connected and technologically advanced society we live in today. Organizations and people are more exposed than ever to cyber-attacks due to the proliferation of digital devices, the advent of cloud computing, and the rising dependence on linked networks. Successful cyberattacks may have catastrophic consequences, including lost money, reputational harm, compromised personal data, and threats to national security. Cyber security strategies have become essential instruments in defending networks, information systems, and sensitive data from hostile actors to counter these threats. To defend against and reduce cyber dangers, a variety of methods, practices, and technology are used in cyber security procedures. These methods work to protect digital assets' confidentiality, integrity, and availability, stop unauthorized access, identify and stop threats, and manage an organization's or people's overall security posture. They play a crucial role in protecting sensitive data, personal devices, online transactions, and vital infrastructure in addition to business networks and infrastructure [1].

Encryption is one of the primary methods of cyber security. Encryption includes using algorithms to transform plain text into cipher text, an unreadable format that preserves data secrecy. Organizations may protect sensitive information, including financial transactions, customer data, and intellectual property, from unauthorized access or interception by putting robust encryption measures in place. When sending data over open networks or storing it in cloud settings, encryption is very important. Another crucial method that confirms the identification of persons or devices trying to access a system is authentication. It makes sure that only authorized people or organizations may access critical materials. Passwords, biometric identification such as fingerprint or face recognition, and two-factor authentication, which combine several verification elements for better security, are common authentication techniques. Effective authentication techniques guard against identity theft and impersonation as well as unauthorized access.

The goal of the access control approach, which is closely connected to authentication, is to manage and limit user rights inside a system. Based on specified rules and user roles, it decides who has access to certain resources, features, or data. Least privilege principles are enforced by access control methods like role-based access control (RBAC) or attribute-based access control (ABAC), which make sure that users only have access to the resources required for their responsibilities. Organizations may lower the danger of unauthorized access and lessen the potential harm brought on by internal or external threats by putting in place effective access control procedures.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Cyberattacks may be detected and mitigated in large part thanks to intrusion detection systems (IDS) and intrusion prevention systems (IPS). IDS keeps track of user activity, network activity, and system activity to look for unusual behaviors or trends that could point to a security violation. IPS, on the other hand, actively prevents or mitigates risks in addition to just detecting them. These systems utilize a mix of behavior-based and signature-based analysis, as well as machine learning algorithms, to recognize well-known attack patterns or find out-of-the-ordinary behavior that could point to a fresh, previously undiscovered danger. Although encryption, authentication, access control, and intrusion detection are fundamental cybersecurity methods, more advanced strategies have emerged as a result of technological improvements. By allowing automated threat identification and response, enhancing human skills, and spotting intricate patterns and abnormalities that could escape the attention of conventional security procedures, machine learning, and artificial intelligence approaches have completely transformed cyber security. By speeding up reaction times and improving threat detection accuracy, these strategies might improve the efficacy and efficiency of cyber security defenses. Furthermore, the use of blockchain technology opens up new possibilities for decentralized and secure data administration. The tamper-resistant and transparent transaction records offered by blockchain, which was first designed for cryptocurrencies like Bitcoin, make it an appealing option for assuring data integrity and trust in a variety of sectors. Due to its distributed architecture, systems are less susceptible to assaults since single points of failure are eliminated [2].

It is a procedure for locating someone and making sure that person is who they say they are. Typically, a username and password are used for online authentication. Due to the rise in reported instances of identity theft through cybercrime, organizations have implemented additional measures for authentication. One of these measures is the One Time Password (OTP), which is a password that can be used only once and is sent to the user via SMS or email at the mobile number or email address that he provided during the registration process. The two-factor authentication technique adds a degree of protection for authentication by requiring two different pieces of identification information. Other well-liked two-way authentication methods include those that combine a login and password with biometric information, physical tokens, etc.

Given that today's international corporations have altered how business was conducted, say, 15 years ago, authentication becomes increasingly crucial. They have locations all over the world, and an employee could need access to information that is stored on a centralized server. Or maybe an employee needs access to a certain file that is on the office network while working remotely from home and without utilizing the intranet. The system must verify the user's identity before granting access to the requested information, depending on the user's credentials. Authorization is the process of granting someone access to certain resources depending on that person's credentials, and it often occurs in tandem with authorization. Since an easy password might result in a security fault and put the whole organization at significant risk, it is now simple to comprehend the need of using strong passwords for permission to secure cyber security. As a result, an organization's password policy should require strong passwords from workers and encourage regular password changes. A hybrid authentication system is used in some larger organizations or in organizations that deal with sensitive information, such as defense agencies, financial institutions, planning commissions, etc. It combines a username and password with hardware security measures, such as biometric systems, etc. Some of the bigger organizations also use VPNs, which are one of the ways to enable hybrid security authentication for secure access to a corporate network over the internet.

Encryption

It is a method of transforming the data into an unintelligible form before sending it over the internet. Only those with access to the key may read it after converting it to readable form. Formally speaking, encryption is a method for locking data by utilizing sophisticated codes created by mathematical algorithms. Even the most powerful computer would need several years to decipher the code due to its complexity. This secure code may be sent securely to the destination via the internet. After receiving the data, the receiver may use the key to decode it. Decryption is the process of utilizing a key to translate a complicated code back to the original text. Symmetric key encryption refers to locking and unlocking data using the same key [3].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

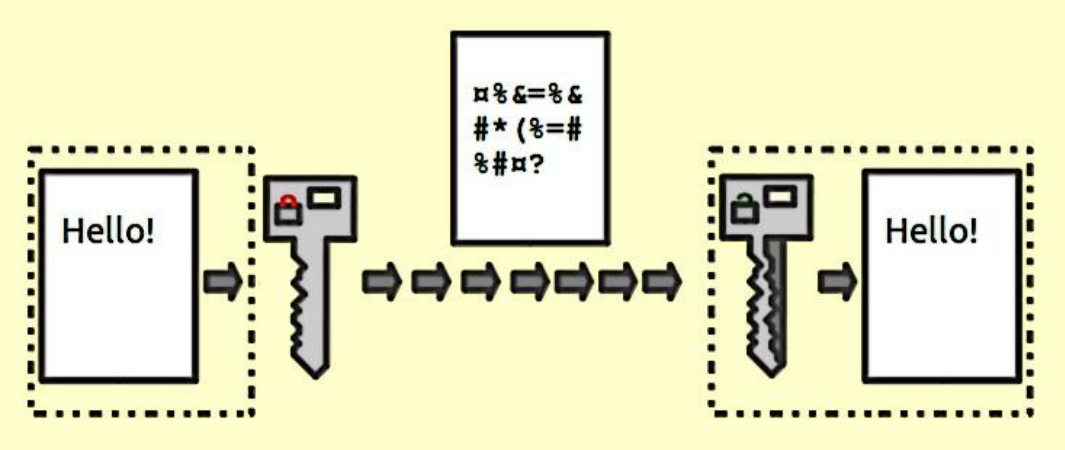

Figure 1: Illustrated the Block Diagram of the Encryption Process

In symmetric key encryption, the key is transferred to the target user through a different means, such as the postal service, telephone, etc., after the data has been encoded since the security of the data is compromised if the key is gained by a hacker. Key distribution is a difficult operation since key security during transmission is a problem in and of itself. Asymmetric key encryption, commonly referred to as public key encryption, is a technique used to prevent the transmission of keys. The keys used to encrypt and decode data are different in asymmetric key encryption. Two keys, namely. Both a public and private key. As the name implies, everyone has access to each user's public key, but only that user's private key is known to them. Let's say sender A wishes to send receiver B a private message via the internet. Since everyone is aware of B's public key, A will use it to encrypt the message. Once the communication has been encrypted, it may be transferred to B securely via the internet. B will immediately use his private key to decode the message after receiving it to recreate the original message [4].

Digital Signatures

It is a method for data validation. A document's content is verified via the validation procedure. Digital signatures are used for authentication as well as data validation. The data is encrypted using the sender's private key to produce the digital signature. Along with the original message, the encrypted data is transferred to the recipient via the Internet. With the sender's public key, the recipient may decode the signature. The original message and the decoded message are now compared. If both are identical, it means that the data has not been tampered with and that the sender's identity has been confirmed. This is because someone who has access to the sender's private key may encrypt the data, which was then decrypted by his public key. Since the data will not be validated, the recipient may quickly identify data tampering during transmission. Additionally, the message cannot be re-encrypted after tampering since this requires the private key, which can only be obtained from the original sender.

Digital signatures are a crucial component of the legal and financial transformation as more and more papers are transferred over the internet. It not only offers the document's validation and the person's verification, but it also stops a subsequent rejection or agreement. Let's say a shareholder sends an email to the broker instructing him or her to sell the share at the present rate. If, once the transaction is complete, the shareholder decides they want their shares back, they may do so by claiming the email is fake or a fraud. The usage of digital signatures helps to avoid these unpleasant circumstances [5].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

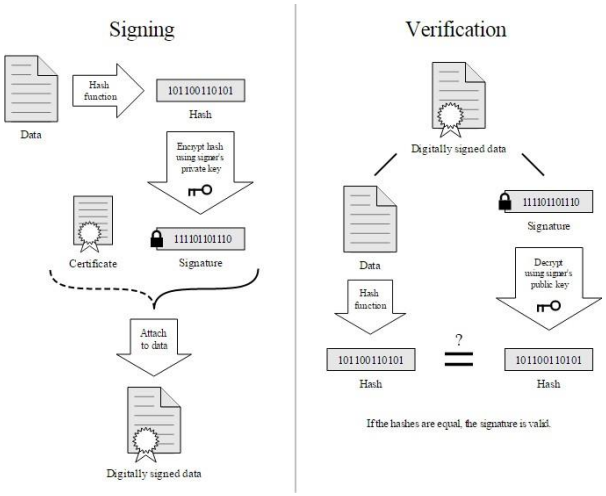

Figure 2: Represented the Block Diagram of Digital Signature

Antivirus

Numerous dangerous programs, such as viruses, worms, trojan horses, etc., are disseminated online to undermine computer security, either to delete data stored there or to make money by sniffing passwords, etc. Anti-virus software, which is a specialized program intended to safeguard the system against viruses, is used to stop these dangerous programs from entering your system. In addition to preventing dangerous code from entering the system, it also finds and removes any bad code that has already been added. Numerous new viruses emerge every day. The antivirus program shields the system against these fresh viruses, worms, and other threats by routinely updating its database.

Firewall

It is a piece of hardware or software that stands between a company's network and the internet and guards against dangers like viruses, malware, hackers, etc. It may be used to restrict who has access to your network and can send you information.

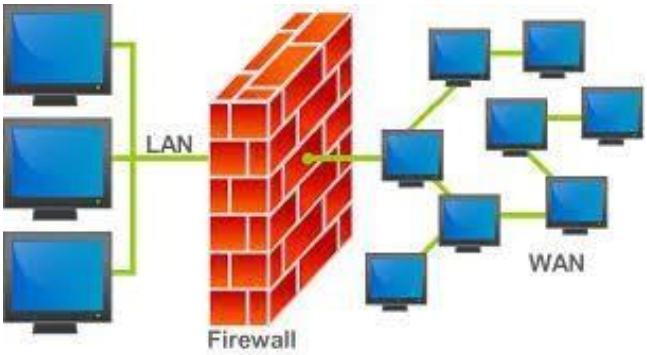

Figure 3: Illustrated the Block Diagram of Firewall

There are two sorts of traffic in an organization viz. both incoming and departing traffic. It is possible to set and keep track of the port traffic using a firewall. Only packets from trustworthy source addresses are permitted to enter the organization's network; untrusted and blacklisted source addresses are not permitted entry. Firewalls are necessary to protect the network from unauthorized access, but this cannot be guaranteed until and until they are set properly. A firewall may be installed using either hardware, software, or a mix of the two [6].

i. **Hardware Firewalls:** An example of hardware firewalls are the routers used to link an organization's network to the Internet.
ii. **Software Firewalls:** These firewalls are placed on the client and server computers and function as a gateway to the network of the organization.

It is included with the operating system in programs like Windows 2003, Windows 2008, etc. The firewall just has to be properly configured by the user under their own needs. The following filtering processes may be applied by the firewalls depending on the "rules" and "policies" that can be specified to be followed by them.

i. **Proxy:** To monitor and manage the packets that are directed outside of the organization, all outgoing traffic is routed via proxies.
ii. **Packet Filtering:** Each packet is filtered based on its type, port information, source & destination information, and the restrictions stated in the policies. Examples of these traits include IP addresses, domain names, port numbers, and protocols, among others. Routers are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

capable of doing fundamental packet filtering.

iii. **Stateful Inspection:** Instead of scanning every field in a packet, important characteristics are identified. Only those specified features are used to evaluate the sent and received packets.

The firewalls are a crucial part of the networks of the organizations. In addition to safeguarding the company against viruses and other harmful code, they also stop hackers from using your network infrastructure to perform denial-of-service assaults.

Steganography

To make the embedded message invisible and retrievable with the use of specialized software, it is a method for concealing secret messages in document files, picture files, programs, or protocols, among other things. The secret message in the picture is hidden from everyone save the sender and the recipient. The benefit of this method is that these files are difficult to detect. Steganography has a wide range of uses, such as hiding communications from prying eyes, shielding private data from theft and unauthorized access, adding digital watermarks to protect intellectual property, etc.

Let's talk about how the data is undetectably inserted into the cover file like the media, such as an image, video, or music, which is used to embed hidden data. Let's utilize an image file used as a cover media as an example. A high-resolution picture is represented by three bytes (or 24 bits) for each pixel. The final picture, once the data is embedded into it, will have a barely perceptible difference in image quality, and only extremely experienced and trained eyes may identify this change if the three least important bits of these 24 bits are changed and utilized for hiding the data. Every pixel may be utilized to conceal three pieces of information in this fashion [7], [8].

DISCUSSION

Cybersecurity solutions are essential for protecting our increasingly digitalized environment from a variety of dangers and weaknesses. Organizations and people must use efficient strategies to safeguard their sensitive data and vital systems due to the fast improvements in technology and the constantly developing nature of cyber threats. By transforming data into a safe format, encryption is a key technology that guarantees the confidentiality and integrity of information. By confirming users' identities and preventing unauthorized access, authentication systems like passwords, biometrics, or two-factor authentication give an additional degree of security. Access control methods reduce the danger of harmful conduct by limiting system access to authorized people. As watchful defenders, intrusion detection systems keep an eye on network activity and spot any intrusions right away. The discovery of abnormalities and trends that human analysts can overlook is another benefit of cutting-edge methodologies like machine learning and artificial intelligence, which improve threat identification and response capabilities. By using blockchain technology, record-keeping becomes decentralized and tamper-proof, supporting data integrity and transparency. However, it's crucial to understand that cyber security relies on more than just technological fixes; it also necessitates people's active participation via security awareness training and adherence to safe coding practices. A comprehensive strategy for cyber security also includes frameworks for risk management, incident response protocols, constant monitoring, and evaluation to keep up with emerging threats. Organizations and people may successfully defend themselves against the constant and evolving cyber threats of our digital era by adopting a multi-layered and proactive strategy [9], [10].

CONCLUSION

In conclusion, cyber security strategies are crucial for protecting against the constantly changing range of online dangers. These methods are the cornerstone of securing information systems and networks, ranging from encryption and authentication to access control and intrusion detection. The methods used to guarantee data confidentiality, integrity, and availability also improve with technology. The use of cutting-edge technology like block chain, artificial intelligence, and machine learning improves cyber security capabilities even further. It is important to realize that technology solutions are not the only factor in cyber security, however. To develop a thorough defense plan, a mix of technological measures, human knowledge, and strong policies are needed. Incident response protocols, risk management frameworks, and ongoing security awareness training are all essential elements. Organizations and individuals may successfully reduce risks, identify dangers, and protect their digital assets in the face of rising cyber threats by using a multi-layered, proactive strategy. To remain

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

one step ahead of the competition and safeguard our digital infrastructure, it is essential to keep up with the most recent developments in the area of cyber security tactics.

REFERENCES

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3041951.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, 2019, doi: 10.1186/s42400-019-0038-7.

[3] M. I. Alghamdi, "Survey on applications of deep learning and machine learning techniques for cyber security," Int. J. Interact. Mob. Technol., 2020, doi: 10.3991/ijim.v14i16.16953.

[4] D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," Int. J. Online Eng., 2017, doi: 10.3991/ijoe.v13i01.6407.

[5] O. U. Oluoha, T. S. Yange, G. E. Okereke, and F. S. Bakpo, "Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey," J. Inf. Secur., 2021, doi: 10.4236/jis.2021.124014.

[6] M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "Security risks in cyber physical systems—A systematic mapping study," Journal of Software: Evolution and Process. 2021. doi: 10.1002/smr.2346.

[7] A. Abdou Hussien, "Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1)," J. Inf. Secur., 2021, doi: 10.4236/jis.2021.121003.

[8] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal, and R. A. Khan, "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," Symmetry (Basel)., 2020, doi: 10.3390/SYM12040664.

[9] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Econ. Financ., 2015, doi: 10.1016/s2212-5671(15)01077-1.

[10] V. B. Savant and R. D. Kasar, "A Review on Network Security and Cryptography," Res. J. Eng. Technol., 2021, doi: 10.52711/2321-581x.2021.00019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Elaboration of Some Recent Cyber Security Attacks

Mr. S Srivinay
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-srivinay@presidencyuniversity.in

ABSTRACT: ***A number of recent cyber security assaults have happened in the online world. We want to learn more about the advancing strategies, methods, and practices used by hostile actors as well as the vulnerabilities exposed by studying these assaults. The research emphasizes how important it is to understand the causes of these assaults and their possible effects on people, organizations, and society as a whole. This study intends to contribute to continuing efforts to strengthen cyber security measures and create efficient remedies against new threats by examining prominent instances, such as data breaches, ransomware attacks, and social engineering vulnerabilities. The results highlight the critical need for effective defense measures, more user knowledge, and cooperative efforts across diverse stakeholders to combat the ever-increasing threats presented by cyber security assaults in our interconnected society.***

KEYWORDS: ***Cyber Security, Data Breaches, Emerging Threats, Malicious Actors, Ransomware Attacks, Vulnerabilities***

INTRODUCTION

Cybersecurity threats are now a constant hazard in today's networked and digitally reliant world, posing a risk to people, businesses, and society as a whole. In order to protect against possible breaches and incursions, continual attention and proactive measures are required due to the dynamic nature of these assaults and the growing complexity of hostile actors. Understanding current cyber security assaults is essential for creating strong defense plans and reducing the dangers brought on by such occurrences. In this study, important recent cyber security assaults that have occurred in the digital sphere are thoroughly examined. We want to learn more about the shifting strategies, methods, and practices used by hostile actors as well as the vulnerabilities they take advantage of by analyzing these instances. This research allows us to identify recurring themes, patterns, and trends that might help us strengthen our cyber defenses and improve overall resilience [1].

One of the major issues in the field of cyber security is the frequency of data breaches. Cybercriminals continue to target businesses of all kinds to steal important financial and personal data. Recent high-profile data breaches, including those that affected significant financial institutions, healthcare organizations, and social media platforms, have shown the far-reaching effects of stolen data. Individuals' confidence is damaged when sensitive personal information is made public, and there is also a serious chance of identity theft, fraud, and other malevolent exploitation. Therefore, it is essential to carefully assess the strategies used by attackers to penetrate networks, exfiltrate data, and profit from stolen information. Attacks using ransomware have also become quite well-known because of how disruptive and expensive they are. Ransomware operations have become noticeably larger and more sophisticated in recent years, focusing on a variety of companies and sectors. Attackers use cutting-edge encryption methods to obstruct access to crucial data and demand large ransom payments in return for the decryption keys. These assaults often cause severe business interruptions, monetary losses, and reputational harm. Analyzing current ransomware events may help organization strengthen their defenses and create efficient incident response strategies by illuminating the attack paths, encryption techniques, and payment methods used by threat actors.

Malicious attackers continue to often use social engineering in addition to technological attacks. Social engineering assaults use psychological tricks and trust-based deception to trick people into giving over private information or allowing unauthorized access. Attackers often utilize phishing emails, impersonation, and pretexting to deceive unwary users. Recent social engineering exploitations have shown how powerful

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

these strategies are, underscoring the need of user awareness and training programs to provide people the information and abilities to see and report suspicious activity. We can understand the motivations and tactics behind current cyber security assaults by digging into the specifics of these instances. This information is essential for creating efficient defenses and putting in place a strong cyber security posture. We may use this information to priorities our resources and efforts by identifying common weaknesses and points of vulnerability.

The populace is using the Internet more and more often every day. The scope of e-governance and e-commerce in the fields of healthcare, banking, electricity distribution, etc. is expanded as a result, however these industries are also exposed to cyber threats including hacking, credential theft, data tampering, account hijacking, etc. In the period from January to May 2014, there were about 62,189 cyber security events, with the majority coming from the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria, and the United Arab Emirates. Additionally, during this period, 10,000 government websites in India were hacked. India is severely lacking in IT security professionals to effectively handle such threats. India needs almost a million cyber security specialists, according to an estimate, to successfully combat online dangers [2].

Some Recent Cyber Crime Incidents

We'll talk about some of the most frequent online fraud and cybercrimes in this part so you can see how even a little ignorance may have a major impact.

i. PayPal is an international online money transfer service that offers an alternative to more conventional payment methods like checks, money orders, etc. by enabling secure online money transfers utilizing a variety of encryption mechanisms. Over 9 million payments are made every day using its active user base of over 100 million users across 190 countries. It is a well-liked method of payment on online auction platforms like eBay and others. It is an easy way to do business, especially when the buyers and sellers are from other nations and use various currencies. As a result, a user may always expect to double their money. Using this loophole, if the user has Rs. 1000, that cash will instantly quadruple to Rs. 2000. In the second try, this Rs. 2000 will be quadrupled to Rs. The additional Rs. 4000 will be multiplied to Rs. Similar to that, this process will never finish.

ii. There is an Australian website called MP3/WMA Land that allows users to download a significant number of illegally obtained songs and music videos for free. For the musicians and the music producers behind those tunes, this led to significant financial losses. An organization named Music Industry Piracy Investigations raised the volume of the complaint.

iii. Mrs. Ritu Kohli reported one of the most intriguing cases of cyber stalking to Delhi Police. She shared her address and phone information after reporting that someone was exploiting her identity to speak on the website www.mirc.com. She therefore got several calls at odd hours from various locations, including Dubai, Ahmedabad, Mumbai, etc. She became quite mentally frustrated by this and decided to file a complaint. Based on her complaint, the Delhi Police tracked the accused's IP address till they located his address and detained him. A NRI living in Dubai was the victim of blackmail, and by the time the incident was reported, he had already paid the accused around Rs. 1.25 crore. The NRI met a female online, and after many lengthy conversations, the girl gained the NRI's affection and trust. She introduces him to a number of her pals in the meantime. The relationship could not survive very long for a number of reasons. After some time, the girl's friend, whom she had introduced to him, informs him that the girl committed herself as a result of the mental stress of the broken relationship, and that the police are looking into the matter. The NRI also received several forgeries of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

letters from the CBI, Punjab University, New York police, High Court of Calcutta, and other institutions. The girl's acquaintance led her to a legal company with offices in Kolkata, and the NRI seemed to be helped by them. The legal firm's proprietor consented to take on this matter. The legal company wanted a large quantity of money, and after many transfers totaling more than 1.26 crore, he continued to seek more money. The NRI saw anything suspicious and informed Mumbai Police of the incident. All of the emails that the girl, her friend, and the owner of the legal company sent to him were forwarded by the NRI. The IP addresses of all three people were discovered to come from the same source during the forensic analysis of the email. Investigation revealed that the girl's and her companions' identities were entirely fictional, meaning that they do not exist. The mastermind behind the scheme to develop this bogus narrative and assume the identities of all the participants in order to extort the NRI was the proprietor of the legal business.

iv. The Stuxnet virus, which is thought to have been produced by the US, targeted Iran's medical facility in Natanz. Since the network of the Iranian nuclear complex is a private network and is cut off from the rest of the world, it was impossible to introduce the virus over the Internet. The malware originally obtained access to the network by infecting a third-party tool used by the Natanz facility. The virus was created to target a certain system program that manages Siemens controller functioning. The centrifuges are sped up or slowed down by the virus, which prematurely wears them down. Additionally, it took control of the system and sent bogus information regarding the condition and status of the nuclear facility. Because of this, the nuclear plant had already suffered significant damage by the time the virus's effects were discovered [3].

v. A trojan email was used to hijack the user identity and password of Mumbai-based company RPG Group's current account, stealing Rs. 2.41 crore via Real Time Gross Settlement (RTGS). When the bank authorities saw the huge money transfer, they had suspicions. They received confirmation of the same from company representatives who had previously denied the movement of funds to the specified accounts. The police discovered that the account holders had given the main accused permission to use their account in exchange for a sizable fee based on the identities and addresses of the account holders who had received the money.

vi. The son of the accused helped two BPO workers boost the credit card limit and the cardholder's communication address, according to a credit card fraud case busted by Chennai police. To get the information about the owner of the credit card, they unlawfully broke into their company's computer. Before the issue was discovered, the credit card firm had been defrauded of roughly 7 lakhs. The owner of a credit card was unable to get monthly statements created at the month's end due to a potential communication address issue. The Chennai police were notified of the incident. Following a digital forensic examination into the BPO's computer system, it was discovered that two of its workers had gained unauthorized access to the system in order to steal client records.

vii. In Andhra Pradesh, a copyright infringement complaint was filed. A well-known mobile service provider firm started a promotional campaign in which it gave its clients a mobile phone at a very cheap price with a 3-year lock-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

in term. The firmware of the phone was set up such that during the lock-in time, any other company's sim cannot be used with the device. In order to "unlock" the phone so that any other sim may be used with it, a rival of that business ensnared the current clients of the business that provided the mobile phone. The business reported the offence, and the copyright infringement action was filed in accordance with section 63 of the copyrights act.

viii. The credit card information of cardholders is stolen from POS machines at shopping centers, gas stations, restaurants and hotels by a cybercrime group, who then use the cards to make online reservations for flights. The findings state that these crooks illegally used over 15000 credit cards to purchase tickets online, resulting in a loss of income of over Rs. 17 crores. To make it harder to track them, these thieves buy these tickets using public infrastructure like computer cafes, etc. The theft was discovered after clients who had been charged for purchasing airline tickets complained to the banks that issued the cards that they had never purchased the tickets in question [4].

ix. A computer virus called the Love Bug worm or VBS/Love letter, which specifically targets computers running the Windows operating system, cost over $20,000 in damage in the year 2000. $22,000 billion. I got a spam email with the subject "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs." If the user opened the attachment, the computer becomes infected, and the worm begins to scan the whole disc and corrupt data. Additionally, it begins sending copies of the emails to every Outlook contact the user has added to their address book. Within minutes, 10% or less of the computers linked to the Internet had been infected. To avoid this worm from infecting their network, several significant organizations, including the British Parliament and the Pentagon, had to shut down their email systems.

x. Nowadays, online degree fraud is quite common, with fraudulent universities offering authorized online degrees. These degree mills promise to convert your professional expertise into a degree in return for payment. Students get transcripts based on their own evaluations as well. He finally realizes that he was a victim of internet fraud when the pupils are turned away due to a bogus degree.

xi. You won't believe how quickly a phone Twitter message may cost $136 billion in losses. In reaction to a false tweet sent from the hacked Associated Press, USA twitter account, which claimed there had been two explosions inside the White House and that President Barack Obama had been wounded, the US financial markets plummeted. Later, the terrorist organization Syrian Electronic Army took ownership of the AP breach on its own Twitter account. A phishing email was used to carry out the breach. When the phishing email's link was clicked, a spyware program was installed on the machine, and the data that was already there was transferred to distant servers. The AP account was compromised using this information, and a fake was produced that affected the investors at the New York Stock Exchange and caused significant loss.

xii. There has recently been a new malware that attacks Point of Sale (POS) systems and steals client credit card payment history. PIN codes, credit card numbers, expiry dates, CCV numbers, and other private information are monitored and given to hackers so that they may use them to execute financial crimes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

xiii. The individuals with bad intents are not only searching for your private and sensitive information; they are also seeking for your communication infrastructure so that they may use you identify to hide their own identity and avoid being caught after causing trouble. The unsecured wi-fi network belonged to US resident Kenneth Haywood, who lives in Mumbai, and was utilized by the terrorist group Indian Mujahideen (IM). Just five minutes before the Ahmedabad explosion, they hacked his wi-fi network and used it to send an email to a news organization that included his IP address [5].

xiv. The terrorist sent a terror email to media outlets using the open wi-fi network of Mumbai's Khalsa College of Arts, Science, and Commerce run by Matsunaga. After utilizing the network, the terrorists remotely accessed the router and wiped the system logs, making it impossible for the investigators to determine where the email originated.

xv. Asma Sandip Throve, a software engineer from Pune, was detained by the economic offences division of the Pune police for stealing the source code of the software product and other private information from Brain Visa Technologies, causing the firm to suffer a loss of Rs. 46.5 crores.

xvi. A brand-new kind of fraud is being perpetrated online where a potential business partner would provide you with a home-based business opportunity that requires no investment and offers a very generous commission. After the individual accepts to work for the organization, the potential business partner will request information such as the person's address, phone numbers, picture identification, birthdate, etc. After some time, a package with repackaging instructions and a list of international addresses to which these packages should be sent will be sent to the person's address. In reality, these items are bought using credit cards that have been stolen, and they are sent to the given address. If the investigators are able to find the address where the products were delivered, the individual will be held accountable. When you get your commission, the real problem starts. The sum is larger than you anticipated and comes in the form of a third-party check. A few days later, a request to electronically repay the extra money is received. The bank will learn that the check is a phoney after the extra money has been transmitted electronically, and the individual will be held accountable for their actions [6].

xvii. A few ICICI Bank clients fell prey to a phishing scam. Some of the clients got an email from someone posing as an ICICI bank representative. He instructed the users to update their account details by clicking on a link that takes them to a page that closely resembles the website of ICICI bank. When some clients became suspicious and alerted the bank's IT department to check the origin of such emails, the bank's authorities reported the case after learning of the fraud. The website's striking resemblance to the bank's official website caught the bank employees off guard. The customer's user ID and password would be sent to the hackers, who could then use them to access the customer's account to make online purchases or transfer money if they utilized the link to update their account credentials on the bogus website.

xviii. Steal the credit card and debit card information, cybercriminals in the US have targeted petrol stations. The majority of the petrol stations in the Southern United States have credit card skimmers that are Bluetooth enabled.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Hackers utilised client data, which includes details like account numbers, PINs, CVVs, etc., to take more than $2 million out of Manhattan-based ATMs.

xix. The US-based female celebrities' private photos were stolen by hackers using technologies that law enforcement uses to analyses data from iPhones. Elkmont Phone Password Breaker and I Brute are said to have been used by the hackers to get into the apple website and download the backup files to their computers

xx. There are several instances when hostile nations undertake cyberattacks to get the private data. One such instance is the suspicion that Russia was involved in the hacking of the US banking system. Russian hackers reportedly assaulted JPMorgan Chase, one of the top banks. The hackers were able to get the private information from the bank's system [7] [8].

xxi. A Chinese cellphone business named Xiaomi was recently found guilty of transmitting private information to Chinese servers. Without the users' awareness, this information includes SMS, pictures, contact information, and more. The US government has prohibited the use of Chinese technology in several of its most important locations, and this is not the first time a Chinese corporation has been linked to espionage suspicions.

DISCUSSION

An extensive study and explanation of the chosen recent cyber security attacks are provided in the discussion section. This investigation reveals a number of significant themes and tendencies. The complexity of harmful actors' strategies, approaches, and processes is one noteworthy discovery. Attackers have developed to take advantage of flaws in a variety of systems, including software flaws, weak passwords, and social engineering mistakes made by users. This highlights the need of using robust authentication systems, remaining current with security updates, and encouraging a culture of cyber awareness and education among users. Data breaches have been a common kind of assault, affecting businesses across many sectors. Sensitive personal information was exposed as a result of these breaches, with serious repercussions for the impacted people and companies. This emphasizes the critical need for strong data protection measures, such as encryption, access limits, and recurring security protocol assessments. Attacks using ransomware have also significantly increased recently. Malicious actors use complex encryption algorithms to lock the files of their victims and demand ransom payments in return for the decryption keys. Organizations may suffer operational interruptions, monetary losses, and reputational harm as a result of these assaults. It emphasizes the need of consistent data backups, efficient incident response strategies, and strong network security to lessen the effects of such assaults. In addition, cyberattacks continue to often use social engineering vulnerabilities. Phishing emails, impersonation, and manipulation strategies play on people's weaknesses by convincing them to divulge private information or allow unauthorized access. Organizations must engage in user training initiatives to improve employees' capacity to see suspicious activity and report it, eventually bolstering the human component of the cyber security defense [9], [10].

CONCLUSION

The analysis of current cyber security incidents indicates the increasing dangers and complexity of the digital environment. Constantly changing their strategies, malicious actors attack organizations across many sectors by taking advantage of flaws in systems. These assaults have a significant effect, resulting in monetary losses, reputational harm, and compromising personal data. Strong defense tactics must be put in place in order to successfully battle these threats, including frequent software upgrades, strict authentication procedures, and data encryption. Additionally, creating a culture of cyber awareness and education is crucial to equipping people with the knowledge and skills they need to spot and counteract social engineering scams. Collaboration between many stakeholders, like as governments, companies, and people, is essential for creating thorough defenses and promoting a safe digital environment. To keep one step ahead of hostile actors and reduce the dangers presented by cyber security threats, continuing research, innovation, and flexibility will be essential

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

as the cyber threat environment continues to change.

REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain," ACM Computing Surveys. 2021. doi: 10.1145/3453158.

[3] V. G. Dharmavaram, "Formjacking attack: Are we safe?," Journal of Financial Crime. 2020. doi: 10.1108/JFC-07-2020-0138.

[4] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," Neurocomputing, 2018, doi: 10.1016/j.neucom.2017.10.009.

[5] Q. He, X. Meng, R. Qu, and R. Xi, "Machine learning-based detection for cyber security attacks on connected and autonomous vehicles," Mathematics, 2020, doi: 10.3390/MATH8081311.

[6] Y. He, F. R. Yu, Z. Wei, and V. Leung, "Trust management for secure cognitive radio vehicular ad hoc networks," Ad Hoc Networks, 2019, doi: 10.1016/j.adhoc.2018.11.006.

[7] D. Zhang, Q. G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," ISA Trans., 2021, doi: 10.1016/j.isatra.2021.01.036.

[8] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances," IEEE/CAA J. Autom. Sin., 2021, doi: 10.1109/JAS.2021.1003820.

[9] T. Hamed, R. Dara, and S. C. Kremer, "Network intrusion detection system based on recursive feature addition and bigram technique," Comput. Secur., 2018, doi: 10.1016/j.cose.2017.10.011.

[10] M. Murphy, "No place to hide as DNS comes under attack," Netw. Secur., 2016, doi: 10.1016/S1353-4858(16)30067-8.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

An Overview of Configuring Firewall on Mac Computer

Ms. Sneha Bagalkot
Assistant Professor, Department of Computer Science & Engineering, Presidency University, Bangalore, India,
Email Id-snehasbagalkot@presidencyuniversity.in

ABSTRACT: ***The process of configuring a firewall on a Mac computer, emphasizing its importance in enhancing security and protecting sensitive information. It discusses the fundamental concepts of firewalls, including their purpose, types, and key functionalities. The abstract further delves into the step-by-step procedure of configuring a firewall on a Mac computer, covering aspects such as accessing the Firewall settings, enabling or disabling it, and customizing the inbound and outbound rules. Additionally, it highlights the significance of regularly updating firewall settings and monitoring network activity to ensure optimal protection against potential threats. Overall, this abstract provides a concise overview of configuring a firewall on a Mac computer, empowering users with the knowledge to safeguard their digital assets effectively.***

KEYWORDS: Computer Accessing, Firewall, Inbound Rules, Network activity, Sensitive Information

INTRODUCTION

In today's interconnected digital world, where threats to our privacy and security lurk at every turn, implementing robust protective measures is of paramount importance. One such crucial defense mechanism is configuring a firewall on a Mac computer. A firewall acts as a virtual shield, fortifying the boundaries between your computer and the vast expanse of the internet, ensuring that only authorized communication flows in and out. By selectively allowing or blocking network traffic based on predefined rules, firewalls play a pivotal role in safeguarding sensitive information, preventing unauthorized access, and mitigating potential cyber threats. Mac computers, renowned for their robust security features, offer built-in firewall capabilities that can be customized to meet individual needs and provide an added layer of defense against malicious entities. This comprehensive guide will take you through the process of configuring a firewall on a Mac computer, equipping you with the knowledge and skills to bolster your digital fortress. From understanding the fundamentals of firewalls to exploring the intricacies of inbound and outbound rules, you will gain insights into how to effectively manage and fine-tune your firewall settings. Additionally, we will delve into the significance of regular updates and network monitoring to stay ahead of emerging threats. By the end of this exploration, you will be empowered to navigate the complex landscape of firewall configuration, harnessing its potential to create a secure and resilient environment for your Mac computer. So, let us embark on this journey to fortify your digital realm and ensure that your personal information remains shielded from harm [1].

Every Mac ship with a built-in firewall a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac? Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.

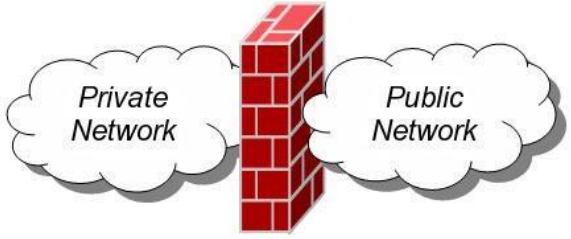

Figure 1: Illustrated the Firewall between Private and Public Network

According to the Figure 1, a firewall can help prevent bad packets from entering your Mac. Hackers love to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans [2].

Working with Windows Firewall in Windows7

i. Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the Windows Firewall, and the other is Windows Firewall with Advanced Security (WFAS). The main difference between them is the complexity of the rule's configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked. Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future [3].

Windows 7 comes with some new features when it comes to firewall. For example, "full- stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces [4]. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

i. Public
ii. Home/Work - private network
iii. Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7 [5].

Configuring Windows Firewall

To open Windows Firewall we can go to Start > Control Panel > Windows Firewall.

Figure 2: Represented the Control Pande Dashboard on Windows Machine.

By default, Windows Firewall is enabled for both private (home or work) and public networks as display in Figure 2. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions, we can go to the menu on the left and select "Allow a program or feature trough Windows Firewall" option.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

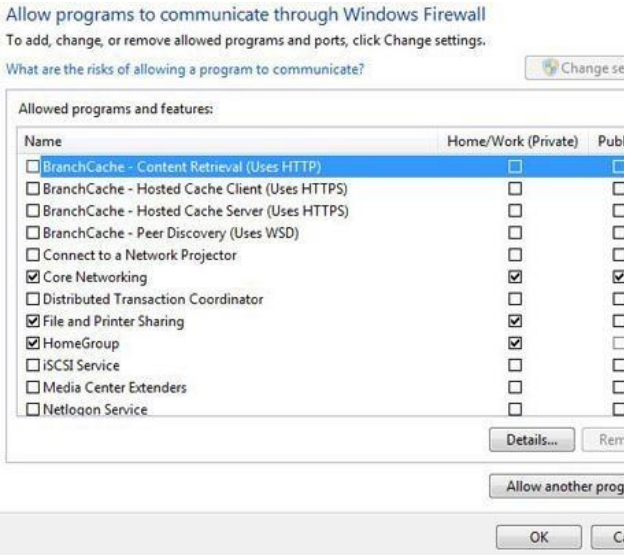

Figure 3: Represented the Configuring Firewall Setting.

To change settings in this window we have to click the "Change settings" button as mentioned in Figure 3. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while File and Printer Sharing is only allowed on private networks, which is displayed in Figure 4. We can also see the details of the items in the list by selecting it and then clicking the Details button [6].

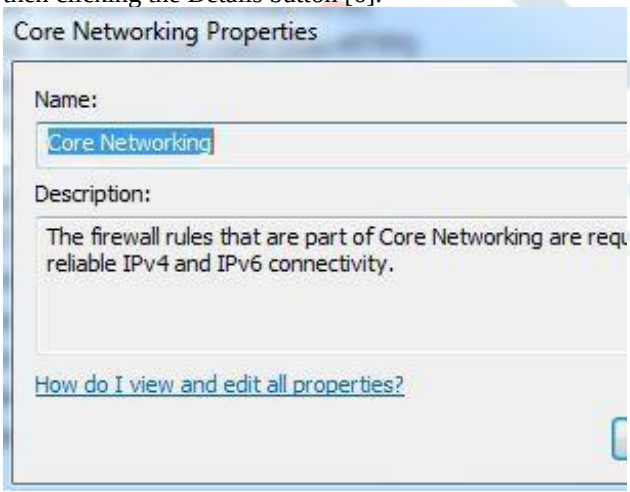

Figure 4: Illustrated the Setting exceptions for Core Networking Properties.

If we have a program on our computer that is not in this list, we can manually add it byclicking on the "Allow another program" button, as display in Figure 5.

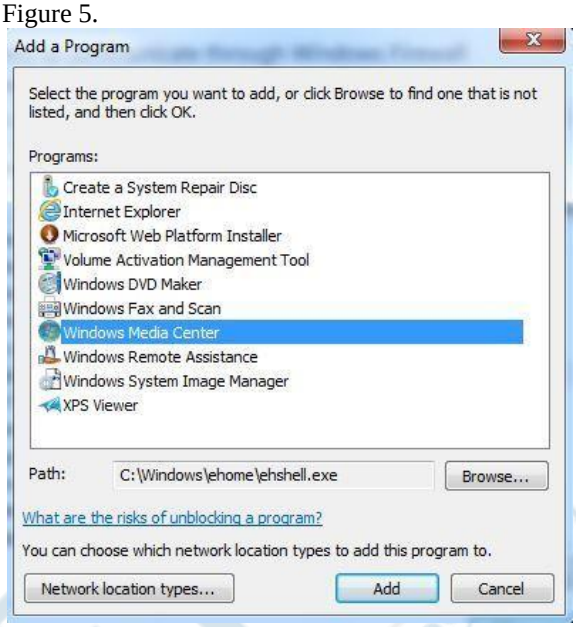

Figure 5: Illustrated the Selecting Programs not Present in the List.

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button as displayed in Figure 6.

Figure 6: Illustrated the Adding a Program.

Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Remote Desktop feature from the system properties window. By enabling Remote Desktop feature, we create an exception in Windows Firewall. Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left mentioned in Figure 6 [7].

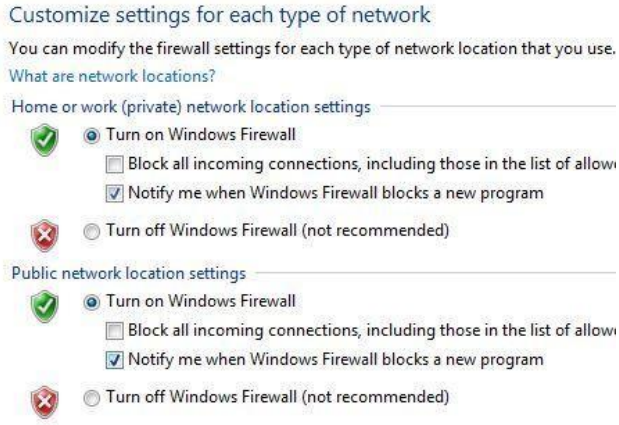

Figure 6: Illustrated the Customize Settings.

Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs. According to the Figure 7, Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

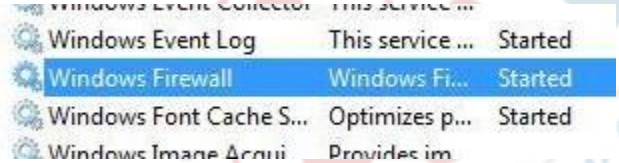

Figure 7: Represented the Enabling Firewall from Windows Services.

Firewall Service

In our case, the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall as in Figure 8.

Figure 8: Illustrated the Firewall notification.

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section [8].

Start & Use the Windows Firewall with Advanced Security

The *Windows Firewall with Advanced Security* is a tool which gives you detailed control overthe rules that are applied by the *Windows Firewall*. You can view all the rules that are used bythe *Windows Firewall*, change their properties, create new rules, or disable existing ones. In this tutorial we will share how to open the *Windows Firewall with Advanced Security*, how to find your way around it, and talk about the types of rules that are available and what kind of traffic they filter.

i. Access the Windows Firewall with Advanced Security

You have several alternatives to opening the Windows Firewall with Advanced Security:

- **a.** One is to open the standard Windows Firewall window, by going to "Control Panel -> System and Security -> Windows Firewall". Then, click or tap Advanced Settings.
- **b.** In Windows 7, another method is to search for the word firewall in the Start Menu search box and click the "Windows Firewall with Advanced Security" result.
- **c.** In Windows 8.1, Windows Firsewall with Advanced Security is not returned in search results and you need to use the first method shared above for opening it.

The Windows Firewall with Advanced Security looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made inWindows 8.1 as displayed in Figure 9.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Figure 9: Illustrated the Windows Firewall with Advanced Security.

Inbound & Outbound Rules

In order to provide the security, you need, the Windows Firewall has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computerto the network or the Internet. These rules can be configured so that they are specific to computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied [9].

In the Windows Firewall with Advanced Security, you can access all rules and edit their properties as display in Figure 10. All you have to do is click or tap the appropriate section in the left-side panel.

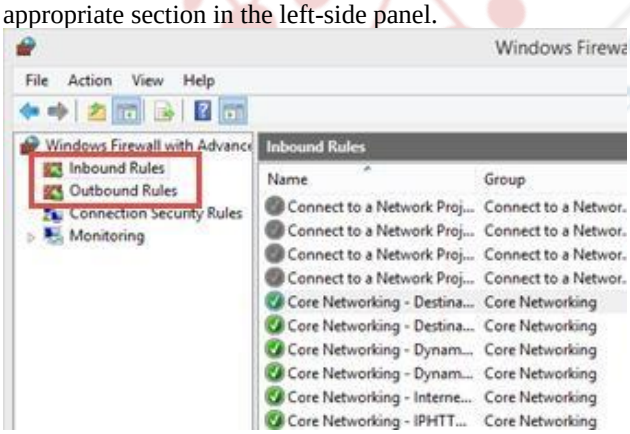

Figure 10: Illustrated the Firewall Inbound Rules

The rules used by the Windows Firewall can be enabled or disabled. The ones which are enabled or active are marked with a green checkbox in the Name column. The ones that are disabled are marked with a gray checkbox. If you want to know more about a specific rule and learn its properties, right-click on it and select Properties or select it and press Properties in the column on the right, which lists the actions that are available for your selection. In the Properties window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.

Connection Security Rules

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted. Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left, as display in Figure 11. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator [10].

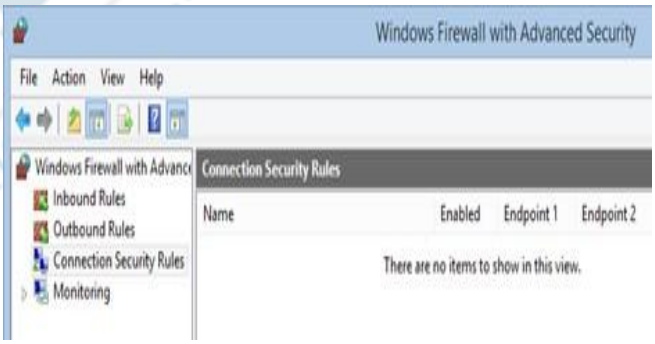

Figure 11: Illustrated the Firewall Security Connection Rules.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

Windows Firewall with Advanced Security Monitor

The Windows Firewall with Advanced Security includes some monitoring features as shown in Figure 12. In the Monitoring section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.

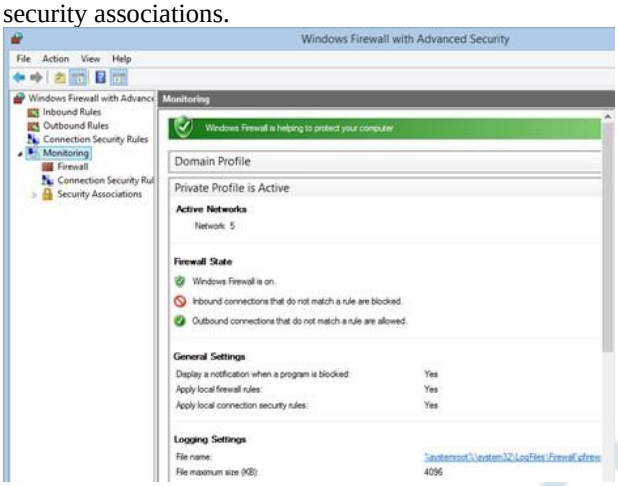

Figure 12: Illustrated the Firewall Monitoring Features.

You should note that the Monitoring section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section. The above section discussed on how to setup a firewall on two Operating Systems viz. Windows and Mac. Linux have many variants therefore it is not possible to discuss how to configure firewall on Linux. There are some links in the Recommended Videos section which discuss the procedure of setting up firewall in various variant of Linux.

DISCUSSION

Configuring a firewall on a Mac computer is a topic that warrants thoughtful discussion due to its significance in protecting sensitive data and ensuring a secure computing environment. The discussion surrounding firewall configuration often revolves around the balance between security and convenience. While firewalls provide essential protection against unauthorized access and malicious activities, they can also introduce potential obstacles for legitimate network communication and software functionality. Therefore, it is crucial to strike a balance between stringent security measures and the seamless operation of essential applications. Moreover, discussing the different types of firewalls available on Mac computers, such as the built-in application-level firewall and third-party alternatives, can help users make informed decisions based on their specific needs and preferences. Additionally, the discussion may encompass the importance of understanding and managing inbound and outbound rules to regulate incoming and outgoing network traffic effectively. Regular monitoring and updates to firewall settings should also be emphasized to keep up with evolving threats and vulnerabilities. By engaging in discussions on configuring firewalls, users can gain insights from each other's experiences, share best practices, and collectively contribute to a safer and more secure computing environment for Mac users worldwide.

CONCLUSION

In conclusion, configuring a firewall on a Mac computer is an essential step towards fortifying one's digital security. By understanding the fundamental concepts of firewalls and taking advantage of the built-in firewall capabilities, Mac users can enhance their defenses against potential cyber threats. This process involves striking a balance between security and convenience, ensuring that legitimate network communication is not unduly hindered. Regular monitoring, updates, and customization of firewall settings are crucial for maintaining an effective defense posture. By actively participating in discussions, sharing knowledge, and staying informed about the latest practices, users can collectively contribute to a safer digital ecosystem. With a properly configured firewall, Mac users can enjoy peace of mind knowing that their sensitive information is shielded from unauthorized access and that their computing environment is safeguarded against malicious entities. So, take the necessary steps to configure your firewall and embark on a journey towards a more secure and resilient Mac experience.

REFERENCES

[1] G. Dorado, S. Gálvez, and M. del P. Dorado, “Computer firewalls: security and privacy protection for Mac—review,” *Big Data Inf. Anal.*, 2021, doi: 10.3934/bdia.2021001.

[2] J. Jain, P. R. Pal, P. Ram Pal, and R. Scholar, “Detecting Worms Based on Data Mining Classification Technique,” *Int. J. Eng. Sci. Comput.*, 2017.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 1S, January 2022

[3] A. Adekotujo, A. Odumabo, A. Adedokun, and O. Aiyeniko, "A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *Int. J. Comput. Appl.*, vol. 176, no. 39, pp. 16–23, Jul. 2020, doi: 10.5120/ijca2020920494.

[4] V. Greiman, "Reflecting on Cyber Governance for a new World Order: An Ontological Approach," *European Conference on Research Methodology for Business and Management Studies*. 2018.

[5] H. Xia and J. Brustoloni, "Detecting and blocking unauthorized access in Wi-Fi networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2004, doi: 10.1007/978-3-540-24693-0_65.

[6] A. Odumabo, A. Ademola, O. Aiyeniko, A. Adekotujo, and A. Adedokun, "ENCRYPTION ALGORITHMS TO SECURE ELECTRONIC MEDICAL RECORDS View project A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS," *Artic. Int. J. Comput. Appl.*, 2020.

[7] Stockholm Environment Institute, "LEAP: Introduction," *LEAP website*, 2020.

[8] D. Pogue, "Mac OS X: the missing manual," *Managing*, 2002.

[9] N. H. Tanner, "Nmap-The Network Mapper," in *Cybersecurity Blue Team Toolkit*, 2019. doi: 10.1002/9781119552963.ch3.

[10] R. Towidjojo, *Mikrotik Kungfu : Kitab 4*. 2015.