IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104015|

CYBER WAR

Dr. Brahmanand Pratap Singh

Associate Professor, Political Science, Pratap Bahadur PG College, Pratapgarh City, Pratapgarh, India

ABSTRACT: cyberwar, also spelled cyber war, also called cyberwarfare or cyber warfare, 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 in order to disrupt, destroy, or deny their use. Cyberwar should not be confused with the terrorist use of cyberspace or with cyberespionage or cybercrime. Even though similar tactics are used in all four types of activities, it is a misinterpretation to define them all as cyberwar. Some states that have engaged in cyberwar may also have engaged in disruptive activities such as cyberespionage, but such activities in themselves do not constitute cyberwar.

Computers and the networks that connect them are collectively known as the domain of cyberspace. Western states depend on cyberspace for the everyday functioning of nearly all aspects of modern society, and developing states are becoming more reliant upon cyberspace every year. Everything modern society needs to function—from critical infrastructures and financial institutions to modes of commerce and tools for national security—depends to some extent upon cyberspace. Therefore, the threat of cyberwar and its purported effects are a source of great concern for governments and militaries around the world, and several serious cyberattacks have taken place that, while not necessarily meeting a strict definition of cyberwar, can serve as an illustration of what might be expected in a real cyberwar of the future.

KEYWORDS: cyber, war, computer, network, internet, crime, government, military, destroy

I. INTRODUCTION

The cyberspace domain is composed of three layers. The first is the physical layer, including hardware, cables, satellites, and other equipment. Without this physical layer, the other layers cannot function. The second is the syntactic layer, which includes the software providing the operating instructions for the physical equipment. The third is the semantic layer and involves human interaction with the information generated by computers and the way that information is perceived and interpreted by its user. All three layers are vulnerable to attack. Cyberwar attacks can be made against the physical infrastructure of cyberspace by using traditional weapons and combat methods. For example, computers can be physically destroyed, their networks can be interfered with or destroyed, and the human users of this physical infrastructure can be suborned, duped, or killed in order to gain physical access to a network or computer. Physical attacks usually occur during conventional conflicts, such as in the North Atlantic Treaty Organization's (NATO's) Operation Allied Force against Yugoslavia in 1999 and in the U.S.-led operation against Iraq in 2003, where communication networks, computer facilities, and telecommunications were damaged or destroyed.[1,2]

Attacks can be made against the syntactic layer by using cyberweapons that destroy, interfere with, corrupt, monitor, or otherwise damage the software operating the computer systems. Such weapons include malware, malicious software such as viruses, trojans, spyware, and worms that can introduce corrupted code into existing software, causing a computer to perform actions or processes unintended by its operator. Other cyberweapons include distributed denial-of-service, or DDoS, attacks, in which attackers, using malware, hijack a large number of computers to create so-called botnets, groups of "zombie" computers that then attack other targeted computers, preventing their proper function. This method was used in cyberattacks against Estonia in April and May 2007 and against Georgia in August 2008. On both occasions it is alleged that Russian hackers, mostly civilians, conducted denial-of-service attacks against key government, financial, media, and commercial Web sites in both countries. These attacks temporarily denied access by the governments and citizens of those countries to key sources of information and to internal and external communications.[3,4]

Finally, semantic cyberattacks, also known as social engineering, manipulate human users' perceptions and interpretations of computer-generated data in order to obtain valuable information (such as passwords, financial details, and classified government information) from the users through fraudulent means. Social-engineering techniques

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104015|

include phishing—in which attackers send seemingly innocuous e-mails to targeted users, inviting them to divulge protected information for apparently legitimate purposes—and baiting, in which malware-infected software is left in a public place in the hope that a target user will find and install it, thus compromising the entire computer system.[5,6]

II. DISCUSSION

In August 2010, for example, fans of the Anglo-Indian movie star Katrina Kaif were lured into accessing a Web site that was supposed to have a revealing photograph of the actress. Once in the site, visitors were automatically forwarded to a well-known social-networking site and asked to enter their login and password. With this information revealed by users, the phishing expedition was successfully completed. An example of baiting involves an incident in 2008 in which a flash memory drive infected with malware was inserted into the USB port of a computer at a U.S. military base in the Middle East. From there the computer code spread through a number of military networks, preparing to transfer data to an unnamed foreign intelligence service, before it was detected. As these above examples suggest, semantic methods are used mostly to conduct espionage and criminal activity.[7,8]

The term *cyberwar* is increasingly controversial. A number of experts in the fields of computer security and international politics question whether the term accurately characterizes the hostile activity occurring in cyberspace. Many suggest that the activities in question can be more accurately described as crime, espionage, or even terrorism but not necessarily as war, since the latter term has important political, legal, and military implications. For example, it is far from apparent that an act of espionage by one state against another via cyberspace equals an act of war—just as traditional methods of espionage have rarely, if ever, led to war. Allegations of Chinese cyberespionage bear this out. A number of countries, including India, Germany, and the United States, believe that they have been victims of Chinese cyber espionage efforts. Nevertheless, while these incidents have been a cause of tension between China and the other countries, they have not damaged overall diplomatic relations. Similarly, criminal acts perpetrated in and from cyberspace by individuals or groups are viewed as a matter for law enforcement rather than the military, though there is evidence to suggest that Russian organized-crime syndicates helped to facilitate the cyberattacks against Georgia in 2008 and that they were hired by either Hamas or Hezbollah to attack Israeli Web sites in January 2009. On the other hand, a cyberattack made by one state against another state, resulting in damage against critical infrastructures such as the electrical grid, air traffic control systems, or financial networks, might legitimately be considered an armed attack if attribution could be proved.[9,10]

Some experts specializing in the laws of armed conflict question the notion that hostile cyberactivities can cause war (though they are more certain about the use of hostile cyberactivities during war). They argue that such activities and techniques do not constitute a new kind of warfare but simply are used as a prelude to, and in conjunction with, traditional methods of warfare. Indeed, in recent years cyberwar has assumed a prominent role in armed conflicts, ranging from the Israeli-Hezbollah conflict in Lebanon in 2006 to the Russian invasion of Georgia in 2008. In these cases cyberattacks were launched by all belligerents before the actual armed conflicts began, and cyberattacks continued long after the shooting stopped, yet it cannot be claimed that the cyberattacks launched before the start of actual hostilities caused the conflicts. Similarly, the cyberattacks against Estonia in 2007 were conducted in the context of a wider political crisis surrounding the removal of a Soviet war memorial from the city centre of Tallinn to its suburbs, causing controversy among ethnic Russians in Estonia and in Russia itself.[11,12]

III. RESULTS

Types of cyber warfare

1. Malware, viruses, and computer worms that can break down a nation's critical infrastructure such as power grids, military systems, critical infrastructures, transportation systems, and water supplies. These systems run on the internet and even if they are well secured, perpetrators are capable of exploiting them.

2. Hacking critical data from businesses, institutions, and governments. Attacking the government's computer systems prevent officials from communicating with each other, enable attackers to steal confidential conversations, steal personal data such as passport information, tax information, etc.

3. Ransomware captures computer systems until the victim pays the ransom. This is usually categorized under disorganized crime wherein the online world's petty criminals come together to plan attacks. Interestingly, these

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104015|

individuals lack technical knowledge and are managing to do well because of the free or low-cost tools available in the market. Their hiring fee is also low as compared to professional hackers who are experts.[11]

Effects of cyber warfare

According to Cybersecurity and Infrastructure Security Agency (CISA), this attack aims to weaken and disrupt the United States of America. For this purpose, unique national Cyberwarfare programs were designed to harm US interests.

National Counterintelligence and Security Center, in its 2018 Foreign Economic Espionage in Cyberspace report, stated that China's Cybersecurity laws have made it mandatory for foreign companies to submit their technology to the Chinese government for scrutiny.

The US's infrastructure has been disrupted to attack its economy or when attacked by the US, its ability to damage another nation has been reduced through Cybersecurity attacks. For instance, controlling a router between supervisory control and data acquisition sensors and controllers in critical infrastructure such as the telecom sector can badly damage the targeted industry.
Cyber attacks are also used to destabilize governments. As per the Report on the Investigation Into Russian Interference In the 2016 Presidential Election, Russia's Internet Research Agency used social media accounts and interest groups to harm the US political system through an 'information warfare'. The effects of Cyberwarfare have been catastrophic for most nations and governments.

Implications of cyber warfare

Cyberspace has been a medium to control military operations, harm business, steal data, and numerous countries have made considerable investments to defend against Cybercrimes. Most nations have witnessed Cyber attacks wherein professional hackers have tried to steal important information and data. [12]

"Hit the computers and you can blackout the airport and the power station in no time as its consequence," states Sourav Mukherjee in his article "Cybercrime and its implications." Attackers start with financial institutions such as banks. The bank balance may drop to zero as a result of a Cyber-attack. Stock prices get moving crazy as a result of hackers leaking data. There have been attempts to jam train signal boards at the railway stations causing a delay in trains' running. The spectrum of Cyberwarfare issues is wide, and it has been predicted that nations may be abridged to congestion and chaos as a result of hackers getting stronger in their attacks.

IV. CONCLUSIONS

Cyber warfare facts

- 95% of breached records in 2016 have come from just three industries that include government, technology, and retail.
- The frequency of a hacker attack is every 39 seconds. Usually, non-secure usernames and passwords allow hackers to attack more easily.
- Most Cyber attacks target small businesses.
- Due to Covid-19, there has been a drastic increase in the reported Cybercrimes as informed by the US FBI.
- Over the past three years, about 93% of healthcare organizations have experienced a data breach.
- Phishing attacks can be best defended through human intelligence and comprehension.
- Unfilled Cybersecurity jobs will reach over 4 million by 2021.
- Human error leads to more than 95% of Cybersecurity breaches.
- Most organizations lack a Cyber Security Incident Response plan.

No organization is safe from an attack that could potentially damage the company's data, reputation, and finances. Nations are paying heaps of money and rewarding information providers about hackers that pose a significant threat to

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104015|

their integrity and state. There are many ways through which nations, organizations, and individuals can reduce their risk of becoming a victim to a Cyberattack.[13]

It is mandatory to protect key infrastructure by keeping in mind that an attack can happen anytime. Nations need to be ready with the right people and resources to prone long term damage, protecting against human shortcomings, and sharing acumen with similar organizations by conducting online workshops about measures to prevent Cyber Warfare. Adopting to hardware authentication, analytics, data loss prevention, machine learning, and cloud techniques help in Cyber Warfare prevention.

Solutions for Cyber Warfare are as follows:

1. Train employees in Cybersecurity measures and principles.
2. Regularly update antispyware and anti-virus on every system used in the business.
3. Firewall connection for the internet.
4. Download software updates regularly for application as they become available.
5. Create backup copies of business information and data.
6. Control access to network components and computers.
7. Secure the Wi-Fi network of your workplace.
8. Track individual user accounts for each employee.
9. Limit employee access to data and information and limit the authority to install the software.
10. Change passwords regularly.

With the expansion of the internet and full use of the World Wide Web (WWW), advanced criminal actions such as internet-driven fraud, Cyberstalking etc. has increased. Technology experts and scholars have advised nations to prioritize and invest in strength for nuclear assault systems and work powerfully towards preventing the nation's critical infrastructure systems. Developing and using a playbook of sorts, can be used in advance to control and guide in responding to a substantial Cyberattack.[14]

REFERENCES

1. Cyber Crime and Cyber Security; tutorialspoint; Date of Access: 30.10.2019 <https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm >
2. The difference between cyber security and cybercrime, and why it matters by Roderick S. Graham; The Conversation; Dated: 19.10.2017; Date of Access: 30.10.2019 < https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654>
3. Understanding the Difference between Cyber Security and Cyber Crime; Privacy International; Date of Access: 30.10.2019 <https://privacyinternational.org/explainer-graphic/2273/understanding-difference-between-cyber-security-and-cyber-crime>
4. Elements of cyber security by Robert Roohparvar; InfoGuard Cyber Security; Dated: 02.03.2019; Date of Access: 30.10.2019 < http://www.infoguardsecurity.com/elements-of-cybersecurity/>
5. Elements of Cyber Security; Cross Domain Solutions; Date of Access: 30.10.2019 < http://www.crossdomainsolutions.com/cyber-security/elements/>
6. Chapter III: Meaning, Concept and Classification of Cyber Crime; Shodhganga; <https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha%5bpter%203.pdf>
7. Types of cyber crime; Panda Security; Dated: 20.08.2018; Date of Access: 30.10.2019 < https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/>
8. Cyber Crime Vs Cyber Security: What Will You Choose?; Europol; Date of Access: 30.10.2019 <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose>
9. Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York.
10. Bowker, Art (2012) "The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century" Charles C. Thomas Publishers, Ltd. Springfield.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104015|

11. Brenner, S. (2007) Law in an Era of Smart Technology, Oxford: Oxford University Press
12. Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)
13. Chang, L.Y. C. (2012) Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait. Cheltenham: Edward Elgar. (ISBN 978-0-85793-667-7)
14. Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details