IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, July 2022

Cyber Warfare: Espionage, Botnet

Mr. Sharan L. Pais, Shrihstha, Shrikara R M, Shruthi C S, Sudheepa Poojari
Department of Information Science and Engineering
Alva's Institute of Engineering and Technology, Mijar, Moodbdri, Karnataka

Abstract: *The essential act of war is destruction, not necessarily of human lives, but of the products of human labour. The topic of cyber warfare is a vast one, with numerous sub topics receiving attention from the research community. We first examine the most basic question of what cyber warfare is, comparing existing definitions to find common ground or disagreements. Recent years have shown us the importance of cybersecurity. Especially, when the matter is national security, it is even more essential and crucial. Increasing cyberattacks, especially between countries in governmental level, created a new term cyber warfare. Creating some rules and regulations for this kind of war is necessary therefore international justice systems are working on it continuously. priority over the last decade, the Human Factors community has yet to approach it with critical mass.*

Keywords: Cyber War, Cyber Warfare, Law.

I. INTRODUCTION

Throughout history, humanity has waged wars, seeking agendas in an ever-changing international power game. of the sword bat- Past tales of today's drone strikes, this power game it is constantly driven to change and evolve by technology. The development of armored vehicles, aircraft, ships and the use of electronics and tele communications expanded the battlespace and introduced new and innovative ways to gain an advantage over opponents. In the early days there were groups that did not set themselves viable goals in and of themselves. Such organizations existed within the physical confines of nation-states, so that attacks against them could only be conducted as part of much broader and more global attacks on the nation-states themselves or the castles and cities in which they were located. . The concept of weakening an enemy by focusing on causing an economic impact other than significant loss of life simply did not exist, and even if military efforts were to focus on disrupting commercial activity, it inevitably implied a focus on killing civilians. In those days, the only means of warfare was kinetic warfare using spears, swords, ballistic weapons, explosives and so on. Non-kinetic warfare, also known as cyber warfare, was not an option as there simply was no digital infrastructure through or against which to leverage attacks.

Cyber warfare refers to the use of technology to launch attacks against nations, governments and citizens, causing damage comparable to real war using weapon. The war continues to spread online known as Cyberwar ,the spread of malicious viruses online can be the future of war. The term “cyberwar is different from the term "cyber warfare". Cyber warfare includes techniques, tactics and procedures, which can be involved during a cyber war.

There are several things about cyberwarfare that differentiate it from hacking for other reasons. Originally, hackers (or "vintage hackers") were people with extraordinary skills and talents, but with typically altruistic motives. It was not uncommon for a hacker to notify the system administrator of a compromised system as soon as a hack was successful, informing him of both how he gained access and how to prevent it in the future. The key motivation was a search for knowledge and greater competence, combined with the lack of a legitimate outlet for one's skills. While their actions were unquestionably illegal there however, a consistent morality existed for these individuals, and they rarely caused the havoc they were capable of.

II. CYBER SPACE

In the following couple of years, the It turns out that the word is clearly related to the Internet computer systems. The term cyberspace is often used to express the Internet contains numerical interaction and communication method. according to the definition of the White House “Cyberspace is made up of hundreds of thousands of computers, servers, interconnected routers, switches, fiber optic cables that allow us critical infrastructure to work. The primary question to ask when examining electronic warfare is: What is cyberspace? Daniel Kuehl [12] looked into this

DOI: 10.48175/IJARSCT-5819

question. Kuehl has collected and analyzed the various definitions offered by a selection of sources, including academic authors, US Department of Defense documents, and even science action. His analysis of existing definitions led him to conclude that cyberspace is more than just computers and digital information, and that there are three aspects of cyberspace that a definition should reflect:

- An Operational space - people and organizations use cyberspace to work and It creates effects, either in cyberspace only or across other domains.
- A natural domain - Cyberspace is a natural domain, made up of magnetic activity and entered using electronic technology.
- Interconnected networks - The existence of connections that allow magnetic activity to carry information.

III. CYBER SECURITY

Protection of frameworks, systems and information in cyberspace against cyber threats needs some kind of security. All the tools, methods, guidelines, activities, and techniques of defend the assets and privacy of users, organizations, agencies Governments called cyber security. The main purpose of Cybersecurity prevents potential security risks for ensure the safety and privacy of important data on the Internet.

IV. CYBER WARFARE

Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponents system is known as cyber warfare. When the system is affected, the entire structure will fall quickly. After attackers infiltrate systems and gain control, anything could happen depending on what type of system was captured. Physical damage, injury even deaths could be possible outcomes due to targeting physical systems controlled by computers. In case of extremely critical infrastructures are invaded by these cyber attacks such as a nuclear reactor can be enormous damage created and would be catastrophic.

V. CONDUCTING CYBER WARFARE

When a new domain of warfare emerges, there is an immediate challenge in resolve. finishing how to operate within it effectively. The arrival of the air as domain From the war researching how to use their property for most people and effectively in it. The same process applies to the arrival of the cyber-do-principal. This research challenge is therefore about how to tackle conduct cyber warfare and how the properties of the cyber domain shape that duct. Parks and Duggan [1] examined the established principles of kinetics war, as defined by the US Department of Defense. They then suggest eight new principles that shape the conduct of cyber warfare**.** These principles are as follows:

5.1 Lack of Physical Limitations

In kinetic warfare, navies must travel across oceans, and land forces must navigate terrain. This does not apply to cyber warfare and an attack can be launched from anywhere with the same impact. This point of view has some arguments against it. means however, as it can be argued that there are still some physical limitations. Just as a navy has to travel on a physical ocean, a cyber attack has to travel through physical wires. The requirement to travel has not been eliminated, It is just the speed of travel that has increased compared to the kinetic forces. in a In the case of delivering malware via USB, physical limitations also apply in get the USB to the required USB port. Where the lack of physical limitations most convincing is in the production of cyber weapons. Traditional weapons they require both materials and time to manufacture - cyber weapons don't have them same requirements and can be replicated quickly and cheaply.

5.2 Kinetic Effects

The purpose of cyber warfare is to cause kinetic effects. This includes physics damage or simply influence the opponent's decision-making process. This view can also be challenged. As our definition states, cyber warfare is the use of warlike cyber attacks. It is not mandatory that the cyber attack is successful and has an effect, only the intent behind the launch it was such a war. This view can be justified by examining some realities world scenarios. Country A fires a missile at country B with the intent to do so destroy a military base, but the missile explodes before reaching

DOI: 10.48175/IJARSCT-5819

its target. IT'S the launch of this missile is not war? Caution should be exercised when requiring kinetic effects to reach a conclusion of cyber warfare.

5.3 Identity and Privileges

The main objective of a cyber attacker is to assume someone's identity who has the access necessary to cause harm. Exploits aim to gain root access, social engineering is designed to collect passwords for privileged users. This is in contrast to traditional warfare, in which assuming identities is not part of the ability to fight the battle. It's hard to argue against this point since then gaining access to privileged accounts is an important aspect of cyber warfare. He does however, ignore some other aspects such as distributed denial of service attacks.

5.4 Dual Use

All cyber warfare tools are dual-use, having both warlike and peaceful uses. This is in contrast to kinetic warfare, where tools are generally single-use. this is The principle has strengths and weaknesses. As a force, it defines it cyber weapons are dual-use. Even tools like distributed denial of service (DDoS) have a peaceful role in testing defenses and improving robustness of the systems. But the idea that dual use is unique to cyber warfare may be challenged. The fact that a computer weapon can be used to test the robustness of a server is not unique to the cyber domain. In the kinetic world, a new tank design will be tested by annular kinetic weapons such as bullets and propelled rockets grenades to test their strength. Kinetic weapons can also be used for hunting, For competitive sport and even for celebration, it rings in the air. And therefore, it can be said that the principle of dual use is not unique to cyber weapons.

5.5 Information as Operational Environment

In kinetic warfare, the physical operating environment must be cross made up of information. In cyber warfare, the operating environment is already information, and does not take any conversion from physical measurements to information place. However, this principle is debatable, since the network that will be used in the Internet prairie war still consists of already existing equipment, objectives attacks can be physical, such as power plants or factories. In this sense, some physical measurements may require conversion to information. looking at the principles presented by Parks and Duggan [22], it becomes clear more work is needed to better identify cyber domain resources that it will shape the conduct of cyber warfare. No physical limitations in cyber weapons manufacturing is the strongest factor identified so far, and it will in fact, who can possess weapons and how many can be produced.

VI. CYBER WARFARE LAW

It is important to know what kind of legal actions it establishes can take globally when they are exposed to such attacks. As said before, cyberspace is a new war and there are still many legal loopholes at the international level cyber attack regulations. Former NSA director, lieutenant The gen. Keith B. Alexander pointed out to members of the senate Armed Services Committee in 2010 that cyber .The war was progressing very quickly and there was “mismatch between our technical capabilities to conduct operations and applicable laws and policies. Teacher Law and Director of the Terror Law Center in St. Mary’s University School of Law Jeffrey F. Addicott has similar perspective. In his opinion international laws associated with the use of force are woefully inadequate in terms of addressing the threat of cyber warfare.

VII. CONCLUSION

The most significant conclusion to be made is that the majority of challenges presented by cyber warfare cannot be solved from the perspective of just one discipline. For example, attribution and cyber defence are certainly technical problems, but political, legal and social input is required to fully resolve these and other issues. Similarly, creating a set of laws for cyber warfare requires not just legal input, but technical and military input on what is feasible to enforce. With this in mind, it must be concluded that a multi-disciplinary method is the best approach future research can adopt. A cyber army for African countries will be an asset to a military force due to the tremendous advancements in technology within the battle space. Cyber warfare is a reality and it will gain a strategic advantage for any nation that

DOI: 10.48175/IJARSCT-5819

has cyber skills, structures, and cyber weapon research and development in place.Cyber warfare is a reality and it is important that there is a cyber army implemented in the African states military with a mandate to execute defensive and offensive actions. A cyber army will ensure that the surfaces and gaps in the cyber space are contained for African nation states to be able to ensure cyber sovereignty.

REFERENCES

[1]. V. D. Cha, "What do they really want? Obama's North Korea conundrum," *The Washington Quarterly*, vol. 32, no. 4, pp. 119–138, Oct. 2009.

[2]. NATO Review Magazine, "Cyber Timeline," in *North Atlantic Treaty Organization*. [Online]. Available: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. Accessed: Feb. 9, 2016.

[3]. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in *IEEE Xplorre*, vol. 9, IEEE, 2011, pp. 49-51. [Online]. Available:http://ieeexplore.ieee.org/stamp/st amp.jsp?tp=&arnumber=5772960. Accessed: Feb. 9, 2016.

[4]. D. Kushner, "The Real Story of Stuxnet," in *IEEE Spectrum*, 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-ofstuxnet. Accessed: Feb. 9, 2016.

[5]. S. J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 2009.

[6]. S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security*, vol. 4, no. 2, pp. 49–60, 2015.

[7]. D. Hollis, "Cyberwar Case Study: Georgia 2008," in *Small War Journal*, 2011.

[8]. J. A. Lewis, "Computer Espionage, Titan Rain and China," Center for Strategic and International Studies, 2005.

[9]. C. Tankard, "Advanced Persistent Threats and how to Monitor and Deter Them," *Network Security*, vol. 2011, no. 8, pp. 16–19, Aug. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485811700861. Accessed: Feb. 10, 2016.

[10]. Google Official Blog, "A New Approach to China," Official Google Blog, 2010. [Online]. Available: https://googleblog.blogspot.com.tr/2010/01/ new-approachto-china.html. Accessed: Feb. 10, 2016

[11]. E. Hanford, "The Cold War of Cyber Espionage," in *Heinonline*, 2014. [Online]. Available: http://heinonline.org/HOL/Page?handle=hei n.journals/pilr20&div=9&g_sent=1&collecti on=journals. Accessed: Feb.10, 2016.

[12]. D. T. Kuehl, Cyberpower and National Security, Potomac Books and 1630 National Defense Univerity, 2009, Ch. From Cyberspace to Cyberpower: Defining the Problem, pp. 24 -42.

[13]. L. Alford, Cyber warfare: A new doctrine and taxonomy, US Air Force, accessed 25/05/14 (April 2001).

DOI: 10.48175/IJARSCT-5819