9 21st Century Threat of Cyber Warfare and Digital Era Security Prospectus

Dr. Omkar Sonawane*
Independent Researcher.

*Corresponding Author: dromkarphd@gmail.com

Abstract

The term cyber warfare has come to light particularly owing to the intensive use of computer and communication technologies. Over the evolution of human beings, we have seen countless bloody conflicts, fought between humans on the issues of nationalism, colonialism, and ideology. On the premise of nationalism, wars were waged on the issues of national interest, on the subjects of trade and navigation rights and fought amongst colonial powers in foreign colonial territories and mainly focused on the different set of ideologies. History shows us since Stone Age, human has relied upon traditional tools and weapons for their survival. This hostility made man to produce powerful weapons in order to safeguard himself, thereby giving him a unique edge within nature. As and when science and technology advances, the quest of discovering new and powerful weapons shall continue.

Keywords: Cyber Warfare, Cyber Space, Cyber Risk, National Security.

Introduction

With the advancement of science and technology, man began to create more powerful weapons, this led to a major shift in the development of weapons technology during the early phases of the 18th century, until the end of the 20th century. Newer weapons of mass destruction were developed and tested. It was at this age when science and technological exploration reached its zenith. In addition, the great European colonial empires fought amongst themselves with the help of these newly developed weapons. While some ushered great success, others failed miserably. This gave an early indication of the importance of science and technology in modern conflict.

The quest for modern weapons continued further and underwent a major revolution with the help of Second Industrial Revolution, where new technology met the capacity of mass production. The Second World War can be said to be the biggest era of display of such modern weaponry. These weapons were not only lethal but also strategic in nature, which could determine the outcome of a battle. At a time when World War was been fought between the Allies and the Axis, in its backstage, the initial development of the computer was found to be crucial.

Further new technological developments and progress were seen during the periods of Great War, which led to the development of the first electromechanical computer. The US Navy was first to use these devices in combat in 1938, as torpedo computers on their submarines. Until then, the computer was never witnessed in battlefields, nor was it used as a war-fighting instrument. It was only during the Second World War that this new computing technology was developed and deployed to decrypt enemies' lines of communication.

After the end of Second World War, computer technology had gained prominence and further progressed, causing a digital revolution coinciding with the advent of the Cold War. The on-going tussle between both the superpowers led to a new era of arms race, which later extended to a space race, thus leading to new technological breakthrough and pioneering technology. Though these technologies were initially non-existent and unimaginable, but with the progress of science and technology and modern computers, many ambitions became reality. The computer was the key to the instrument in developing these new technologies, which not only led to mass production but also increased speed, output, efficiency, accuracy, precision along with strategic impact, which otherwise would otherwise have never been thought off. Such reliability, speed and precision offered by computers prompted all command-and-control communication systems to shift from war room towards computer without getting into the need for complex decision-making process.

Nation-states of the 21st century clearly understand and perceive that the modern dependency on computers and the Internet has now become a liability. This liability and dependence on cyber space shall now be subject to cyber-attacks of tomorrow in order to collect and steal information on the adversary's capabilities and vulnerabilities, which shall seek to destroy its functionality or to retaliate in case of war. It is to be noted that in cyber space, offence dominates defence. Thus, cyber warfare is the action of a nation-state in order to infiltrate the enemy's computer network, conduct espionage, destroy critical information systems, disrupt critical infrastructure, command & control systems, communication satellites, government and military databases along with strategic institutions.

Cyber warfare: The New Threat to Nation-State

In simple words, cyber warfare is the use of computer technology by a nation-state in order to direct cyber-attacks against the adversary to potentially harm or destroy its computers, networks, which coordinate military and civilian systems. Such attacks are a matter of concern, especially in areas of command-and-control, defence networks, guided weapons systems, which need C3 to operate.

The impact of cyber warfare on national security is such that the government institutions and private organisations must work together to counter the emerging threat of cyber warfare in cyberspace. Cyber warfare is at its best when cyber-attack takes place without the knowledge of the enemy. Thus, cyber warfare is the new subset of information warfare, wherein nation-states are forced to evaluate their military strategies along with strategic thinkers, who need to develop new mitigation strategies in order to their protect nation states sovereignty in cyberspace just like it would be the case for land, sea, air, and space.

Further, cyber warfare also extends to the private entities and individuals who regularly face cyber-attacks from the attackers in order to steal and gain access to critical information in areas of research and development, high-performance technologies, defence technology, trade secrets, weapon designs, intellectual property, arms manufacturing companies, military databases, deep space research, telecommunications sector, airways and railways sectors, private email accounts of important dignitaries and large multinational corporations. Thus, the threat of cyber warfare is real and immediate.

- **Correlation of Cyber Space and Cyber Warfare**

The term "cyberspace" first appeared in a science fiction novel wherein the word is derived from Greek word ‘cybernetics’, which means' one who governs’, and its modern definition was described in a 1948 book by Norbert Wiener, which describes the study of command and control and communication in the mechanical world. In contrast to land, sea, air, and space, cyberspace is neither a naturally occurring phenomenon nor can it exist without information technology and electromagnetic spectrum.

Cyberspace is neither concrete nor physical as compared to physical spaces, which have volume, depth and gravity causing direct impact upon humans. Cyberspace encompasses computer networks, where its endpoints are connected to the larger networks, which form the building block of cyberspace, and are formed, by connecting to these networks with electromagnetic spectrum. Cyber Space builds on these information networks that include the physical aspect of cyberspace. These physical components comprise EMS and IT infrastructure, both hardware and software, which are essential to establish cyberspace.

- **Layers of Cyber Space**

To briefly understand the cyber space, one needs to know about the layers of cyber space which includes;

  - Hardware is the *first layer of cyberspace.* It includes: circuits, processors, microchips, storage devices, input and output devices, communication equipment, wireless technology, routers, servers, fibre optics, undersea cables, transistors, and receivers that form the building blocks of cyberspace.
  - The *second layer comprises* software, through which physical IT infrastructure is guided and controlled. Computer programming and coding are key to the development of such software.

- The *third layer* which consists of information is crucial to the existence of cyberspace. Data is raw information, which is stored in computer storage devices, networks, the cloud, and servers. These systems often rely upon information technology and internet in order to communicate with other networks.

The ability to reprogram targets of a weapon system, which relies on real-time information from military networks or satellites for a precision strike, would not been imaginable without the active use of computer, information technology and cyberspace.

- **Characteristics**
  - Without the current existing EMS, cyberspace would not have been possible. Millions of ICT devices would not be able to communicate with each other and neither would internet exist. Furthermore, electrons are essential to control integrated circuits and electronic devices of a computer.
  - Cyberspace, with its unique character unlike other naturally occurring physical domains, i.e., land, sea, air, and space, requires manmade object to exist. Cyber space would not have existed without the human's ability to innovate.
  - Cyber space is easier to expand as computer and network hardware are easily available and can be repaired if damaged, thus providing a limitless supply to cyber space.
  - Access to cyberspace is relatively cost-effective compared to the other physical domains, as it requires minimal resources and expertise are required in comparison to the physical domain.
  - Strategic impact on cyberspace can be achieved with minimal resources, where modest financial investment, along with a group of technically trained individuals who have the ability to hack into computer networks.
  - Offensive cyber warfare dominates cyberspace because of several reasons. First, a cyber defence system relies upon IT systems, which are often outsourced and vulnerable to open architecture followed by weak protocols. Second, cyber-attacks occur at lightning speed, putting an onus on the defender to defend computer networks against cyber-attacks. Third attack that originates in cyberspace, reduces geographical constraints and physical barriers between nation states.
- **Characteristics of Cyber Warfare**
  - It is the asymmetric nature of cyber warfare wherein cyber-attack are carried out against an adversary at minimal costs. Also, the positing of cyber-attacks in the escalatory ladder of conflicts still remains unclear,

which could be well situated from the lower realms of the spectrum to the upper ends of strategic conflict.

- The level of anonymity remains high, as it is difficult to detect the source of the cyber-attack and is often time-consuming to identify its perpetrators.
- Cyber warfare is the actions wherein cyber intrusions are extensively been done in order to gain access to a computer, computer network, military intelligence, intellectual property and critical information systems.
- Cyber Warfare has cross-domain linkages wherein cyber-attack against the target in a particular sphere may result in cross-sectorial disruption, where attacks on critical infrastructure like power grids, transportation networks, financial systems and information and communication technology can have direct consequences on national security.
- Further, cyber warfare targets includes; command and control, critical information systems, decision support systems, navigation systems, outer space assets, precision-guided weapons systems, critical infrastructure and industrial control systems. Hence, cyber warfare is an emerging aspect of warfare, which is needs to be understood in detail, and shall be further studied, by understanding its different forms

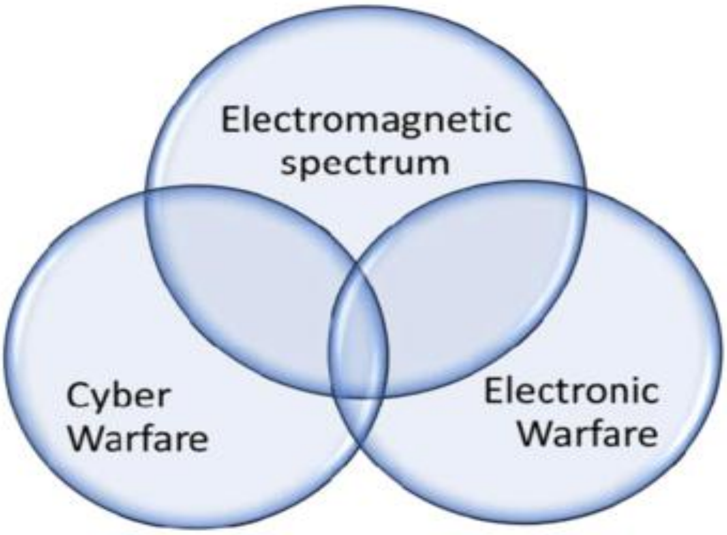

Figure 1: Cyber Warfare Ecosystem

Key Areas of Cyber Warfare

Cyber Warfare in the 21st century largely involves the use of information technology in order to gain access to information networks that control and operate cyberspace. Also, new operational concepts like Information Warfare, Hacker Warfare, Cyber Warfare, Command and Control Warfare and Cyber espionage would not have been possible without such cyber ecosystems.

- **Electronic Warfare**

Electronic warfare is a type of information warfare in which electronic weapons are used to adversely affect the adversary’s communication systems and weapons systems, as well as to affect its combat capability. Electronic warfare is defined as a military tactic that uses electromagnetic spectrum and focused energy to control and manage events in the electromagnetic spectrum. It also includes launching an electronic attack against the adversary and its battle equipment. Electronic warfare is a military activity aiming to control the electromagnetic spectrum in an act of war. As a result, electronic warfare is a collection of military actions whose primary role is to maintain control over electromagnetic space, which is its key domain.

- **Command and Control Warfare**

Command and control warfare is a term that has been used by the US Department of War to describe combat. C2 warfare is a military strategy that attacks and removes the command-and-control structure of the opponents from the units they command in field operations. Depending upon the nature of tactical and strategic objectives, defusing is generally accomplished by injuring the battle commander or damaging the communication channel. Finding the command post is more crucial than locating a commander's physical position, as attacking the command and control can have serious operational consequences and obviates the need for the opponent to be neutralized. In most cases, the command post is intangible in the opponent's overall structure, and its eradication is rarely overlooked.

- **Hackers Warfare**

Hacker warfare is a type of information warfare, wherein a skilled hacking professional carries out systemic cyber-attacks. Hacker's warfare usually aims to cause network congestion through the distributed denial of service attack, or deface targeted websites through web defacement strategy, or carrying out advanced persistent threat attacks against adversaries. Computer systems that appear appealing to the hacker are its primary targets due to its financial and informational value. Hacker warfare can be further defined as a series of organised large-scale cyber-attacks that have strategic outcomes.

Such hackers could be non-state actors which includes hacktivist, terrorist groups, insiders, corporate groups, mercenary and rogue nation states, whose actions are often difficult to detect and track. Hacker Warfare relies upon powerful computing technology, artificial intelligence along with advanced cyber tools to carry out sophisticated cyber-attacks in cyber space. Its targets include internet users to corporate entities, government employees posted in sensitive location, and senior organisational employees holding prominent positions such CEO, CFO and COO, who are subject to advanced persistent threat attacks. The impact of hacker warfare is inversely proportional to the degree of computer and computer network integration within a given network. Hacker warfare has been largely successfully where countries have weak cyber laws along poor law enforcement and detection.

- **Information Warfare**

The term information warfare refers to a type of warfare that is guided by information. Data along with Metadata in the form of numerous defence contracts, list of defence contractors, business development strategies, intellectual property, trade secrets, patents, internal structure of the organisation, research and development, scientific invention, production plans, manufacturing plants, production faculties, strategic institutions, legislative practices and offshore financial investments data can all be considered critical information. It is clear in a global interdependent context, that there is perpetual confrontation between various intelligence and financial agencies, and corporate agencies involved in corporate espionage and fight between nation states over control of information, which could be obtained by committing industrial espionage, cyber espionage and computer hacking. For example, over the recent course of years, spyware attacks carried out against multinational tech giant IBM, Japanese business Hitachi, is alleged to steal secret information worth billions of dollars.

- **Psychological Warfare**

Psychological warfare involves the use of propaganda tactics in order to reduce the enemy's morale and mental wellbeing. Psychological warfare does not resort to the use of violence; rather it uses psychological tactics and techniques of ideas, memory distortions, and manipulation of facts, mis-information and mal-information in a deliberate manner to spread disinformation amongst the masses, in order to influence their political and legal opinions. Propaganda involves the art of spreading disinformation in order to protect and promote one's political interests against the enemy's.

Table 1: Principles of Warfare

Selection and Maintenance of Aim	The aim is expressed as an intention, purpose, or end state. It should be selected and defined clearly and must be simple and direct.
Objective	Direct military action towards a clearly defined and attainable objective.
Morale	High morale fosters offensive spirit and will to win.
Offensive Action	Offensive action is the chief means of achieving victory. It results from offensive spirit and helps to maintain initiative.
Surprise	Catching the enemy off guard, thereby forcing one to lose control.
Flexibility	Capability to react appropriately to a changing or dynamic situation.
Intelligence	Intelligence involves acquiring information on the enemy. Intelligence is advanced information and plays a crucial role to ensure deceive outcome.
Strategy	Placing the resources at the right places and right time to achieve battle's objective.

Source: Created by Author

Propaganda is one of the key tactics that is used in psychological warfare. Modern methods of psychological warfare include; fake news, AI deep fakes, spreading mis-information and disinformation on digital platforms and social media networks along with suspicious micro blogging to promote violence.

Summary

It involves the role of a nation-state to carry out a cyber-attack against the adversary. Hackers who work on behalf of the government are highly trained cyber security professionals who do the job of state sponsored hacking when required. Such technocrats are often raised in troops on the lines of nationalism. They target other nation states, business organisations, non-state actors and prominent individuals. Cyber-attacks have been carried out in order to gain access to information that is critical and has international significance.

Nation states precisely know as to what they are getting into and are fully aware of the consequences, but despite these shortcomings, they choose to attack the adversary in cyber space in to order to gain access to their computer systems and network. As these cyber-attacks are being funded by the state and are being carried outside enemies' territorial jurisdiction, there is the least likelihood of such cyber criminals being arrested or prosecuted in the court of law. Even if such cyber acts are investigated, nation states may not accept the ownership of such acts.

Similarly, nation states may also conduct cyber surveillance of their citizens living abroad, who may have either fled their country due political threats or do not acknowledge its current political regime. State sponsored hackers are given necessary tools, technology needed, and authority to carry out a cyber-attack from within state's borders. In an act of war, nation-states may attempt to gain access to the enemies' critical infrastructure system and could launch a cyber-attack when directed by government. Nation states may also deploy hackers in cyber space to conduct cyber espionage, by attempting to steal vital information, industrial secrets, classified information from various governments and their departments and international businesses, disrupt critical infrastructure services, targeting multinational companies and promote propaganda through disinformation.

Hacktivists are politically motivated individuals who hack into computer systems and government networks for political and social reasons. These hackers hack into government organizations and businesses in order to dis-credit them by publishing sensitive information about its workings in the public domain. The key objective of such groups is to cause damage to the reputation of organisations or government in order to seek international attention.

A financially motivated employee will act in a similar manner as a disgruntled employee, but for financial gains. Such an employee would steal company data and pass it on to the competitor for financial gains. Such uncalled behaviour would cause a setback to the company's integrity and confidentiality of its data. If an employee's behaviour goes unnoticed for longer periods, then it could damage the company's market and clientele on grounds of lack of professionalism and importantly, confidentiality. Similarly, a disgruntled employee is an individual who is dissatisfied with the job or terribly upset with its boss's relationship. The dis-grunted employee could take revenge by dumping classified information into the public domain or pass such information to the organizations competitors.

Conclusion

As discussed in this chapter, computing technology advances, the need to access information shall only continue to increase and become an enviable part of everyday life. The need to access the system of information along with its protection have made information security and cyber defence essential, particularly in the light of threats such as malicious malware, cyber-attacks, and hackers' warfare.

Critical infrastructures today, are managed by centrally coordinated information systems and cyber infrastructure. Therefore, the security of these critical infrastructures is unique given the increasing complexity of challenges in present times. The growing cyber-attacks of today are now increasingly being perceived as a major threat to these systems of critical infrastructure. Such cyber-attack have the destructive capability and potential to cause significant damage to the computer networks and critical infrastructure, resulting it in catastrophic loss, data loss, loss of human lives, data theft, and malfunctioning of these systems as a whole.

Cyber-attacks are threats that not only affect those computers online but also extend to offline computer networks wherein they can disable a country's power grids, thereby affecting financial and banking systems. Critical infrastructure has become the popular target of cyber attackers over the past few years. Critical infrastructure can be defined as computer systems that have national significance and are vital to nation building. It acts as a backbone to the nation's core infrastructure and provides essential support system to economy, polity, and security; often making it as an intangible asset of national security. Critical Infrastructure includes: electricity, water supply, sewage management systems, nuclear facilities, healthcare systems, information technology and national informatics. These critical systems are managed with the help of industrial control systems.

References

1. Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US efforts to Secure the Information Age. New York: Routledge.
2. Chaudhary, C. K. Stories of Cyber Crime & Protection Mantra. Chennai: Notion Press.
3. Chen, T. M. (2014). Cyberterrorism (L. Jarvis & S. Macdonald, Eds.). New York: Springer.
4. Colarik, A. M., & Janczewski, L. J. (2007). Cyber Warfare and Cyber Terrorism (Premier Reference). United States of America: Information Science Reference.
5. Dr. Sharanjit. (2014). Anti-Terror Laws in India. New Delhi: Regal Publications.
6. Erbschloe, M. (2001). Information warfare. New York: McGraw-Hill Osborne Media.
7. Ferraro, P. (2016). Cyber Security (1st ed.). Hasmark Publishing.
8. Fotion, N., Kashnikov, B., & Lekea, J. Terrorism: The New World Disorder (1st South Asian). Chennai: Continuum International Publishing Group.
9. Gaber, H. (2020). 2020 Cyber Security and Cyber Law Guide. Edmonton: HSM Press.

10. Hicklin, J., Shurvinton, B., & Beard, G. (2015). The Internet of Things for Dummies. England: John Wiley & Sons,Ltd.
11. Huda, S. (2019). Next Level Cyber Security Detect The Signals Stop The Hack. Levanto: Leaders Press.
12. Jain, D. A. Cirminology: Penology & Victimology (3rd ed.). Delhi: Ascent Publication.
13. Johnson, T. A. (2015). Cybersecurity. Boca Raton: CRC Press.
14. Karthikeyan, M. (2017). Internal Security by Pearson (2nd ed.). Pearson India Education Services Pvt. Ltd.
15. Khosla, M. (2012). Indian Constitution. New Delhi: OUP India.
16. Kshetri, Nir. (2013). Cybercrime and Cybersecurity in the Global South (1st ed.). Palgrave Macmillan.
17. Lutz, J. M., & Lutz, B. (2011). Terrorism. New York: Taylor & Francis US.
18. Mitra, A. (2008). Digital Security Cyber Terror and Cyber Security. New York: Infobase Publishing.
19. N, D. M. (2015). Cyber Terrorism and Information Warfare (1st ed.). Delhi: Vij Books India Pvt Ltd.
20. Pandey, Dr. O. N., Aneja, B., & Pandey, N. (2016). Cyber Security (1st ed.).
21. Paranjpe, S. (2009). India’s internal security. Delhi: Kalinga Publications.