International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Warfare and it's Impact

Abitha Sangamithra A

B. Com LLB (Hons), Dr. Ambedkar law university Tamilnadu, Chennai

ABSTRACT:

Cyberwar refers to digital attacks like hacking, computer viruses by one nation-state over another nation in order to cause damage, death and destruction. However, some actions of cyber warfare may include non-state actors, such as terrorists, activist group or a nations citizen either as the attackers or targets. Unlike conventional weapons and troops these are modern-age war in the digital era and could cause much bigger damage to a country than traditional war. This paper focuses on the concept of cyber warfare and the forms in which cyber warfare can be waged. Some of the forms are Espionage, DDoS, Propaganda attacks, Data theft, Hacking. The paper also elucidates the effects of cyberwarfare over a country like Disrupt essential government services, Influence on the stock market, Influencing opinions, Conflict among nations. This paper examines India's current approach and initiatives towards cyber security. To further understand the concept of cyber warfare this paper will then discuss some real cyber-attacks over the years.

Keywords: Cyber warfare, digital era, espionage, cyber space, hacking

1. INTRODUCTION:

The internet has to be considered a very dangerous battlefield. The countries that don't feel vulnerable are the most threatened by cyber war, such an attack is cheaper than conventional methods of war which includes weapons and armed forces. Cyber warfare is an extension of policy by actions taken in cyber space by state or no state actors that constitute a serious threat to the nation's security. It is obvious from the military standpoint that cyberattack and defence against them has to be an indispensable part of military activities. Cyber warfare has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems.

2. CYBER WARFARE:

Cyber warfare is a form of war in the new digital era, it is a type of network or computer-based conflict in which a nation-state or international organization attacks or attempt to damage another nation through a series of cyber-attacks which has the capacity to wreck and cause serious damage to the targeted country. Cyber warfare is different from cyber war in that cyber warfare typically refers to the techniques involved in engaging cyber war. Cyber warfare generally attacks a country's financial infrastructure, public infrastructure, banking system, safety and military resources.

Parks and Duggan focused on analysing cyberwarfare in terms of computer networks and pointed out that "Cyberwarfare is a combination of computer network attack and defence and special technical operations.[1]

Taddeo offered the following definition in 2012:

The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances.[2]

Cyber space: Cyberspace is a dynamic and virtual space that such networks of machine-clones create. In other words, cyberspace is the web of consumer electronics, computers, communications network which interconnect the world.

Cyber Crime: A crime committed where the use or knowledge of computer is required to cause damage is Cyber Crime.[3]

Cyber Security: Cyber Security is the evolution of policies and procedures to protect own information and information system.

3. FORMS IN WHICH CYBERWARFARE CAN BE WAGED:

Espionage

Cyber espionage is an act of intrusion which can provide the information needed. Traditional espionage is not an act of war, nor is cyberespionage, and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations and are often described as "attacks".

For example:

(i) Massive spying by the US on many countries, revealed by Edward Snowden.

(ii) After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi (the official state security service of the German Democratic Republic)

DDoS:

Distributed denial of service attack (DDoS), it makes computers inaccessible to target users. DDoS attacks computers or network with weak security systems. This type of attack can be used to disrupt critical operations and systems and block access to sensitive websites by civilians, military or research bodies.

Propaganda attacks:

The aim of propaganda is to control information and influence public opinion. Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion. It is a form of psychological warfare, except it uses social media, fake news websites and other digital means. Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist. The internet is a phenomenal means of communication. People can get their message across to a huge audience. Terrorist organizations use this medium to effectively to brainwash people and also recruit potential members.[4]

Data theft:

Hackers of computer systems steal information that can be used for intelligence purposes, held for ransom, sold, or even destroyed.

Hacking:

Hacking critical networks could enable the attackers to extract important information from government, institutions etc.

4. EFFECTS OF CYBERWARFARE:

Cyberwarfare has led to cause physical destruction and loss of life. In today’s word where everything is socially connected cyberwarfare may cause problems in essential government services such as health care, financial services etc. It also leads to cause an influence in the stock market and causes to fluctuate the stock prices as a result of hackers leaking data. Cyberwarfare has become a threat to the national security of a country and creating conflict among nations, cyberwarfare could be both offensive and defensive.

5. INDIA’S SOPHISTICATION:

India is positioned among third-tier countries on the spectrum of cyberwarfare capabilities. This position is determined by the country’s strength on digital economics and the level of intelligence and security and how well cyber facilities are integrated in military operations. Unlike other countries India lack a modern, comprehensive cyberwarfare strategy.

India has taken steps in establishing institutions and released the National Cyber Policy in 2013 to deal with cyber security issues. In recent times, India has launched a series of cyber security initiatives to digitally empower its citizens and safeguard cyberspace. In the wake of increasing cyber threats, India appointed its first chief information security officer (CISO). The appointment underlines India’s commitment to combating cyber attacks. It will help India develop the vision and policy to fight cybercrime and manage cybersecurity more effectively.[5]

Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. This includes National Cyber Security policy (2013), Framework for enhancing Cyber Security (2013), enactment of Information Technology (IT) Act, 2000 and setting up of Indian Computer Emergency Response Team10 (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000.

The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber-attacks from outside the country, periodic scanning of cyber space is carried out. CERT-In has issued 372, 402 and 432 advisories during 2014, 2015 and 2016 respectively.

In May 2021, India set up its Defence Cyber Agency (DCA). The DCA works closely with National Technological Research Organisation, India’s Research and Analysis Wing, National Security Council, and the Defence Research and Development Organisation. These organisations have often been the target of cyber-attacks and are now protected to a greater capacity with the inclusion of the DCA. The DCA aims to thwart any attacks on their authorities to access critical military infrastructure.[6]

6. INTERNATIONAL COLLABRATION OF CYBER SECURITY:

i. India and the U.S. agreed to cooperate on cyber security issues. As a part of the U.S.-India Cyber Relationship Framework, both countries agreed to share cyber security best practices, share threat information on a real-time basis, promote cooperation between law enforcement agencies and encourage collaboration in the field of cyber security research. India and the U.S. will also establish joint mechanisms to mitigate cyber threats and protect internet infrastructure and information.

ii. In 2015, India and the U.K. made a joint statement about cooperation in the cyber security space. The two countries agreed to work together to provide professional development and establish a Cyber Security Training Centre of Excellence. The U.K. also agreed to help launch the proposed National Cyber Crime Coordination Centre in India.[7]

iii. India has entered into cyber security cooperation with European Union and Malaysia

iv. India and Japan are collaborating on cyber security in the form of Memorandum of Understanding (MoU) signed between CERT-In and Japan-CERT in 2015 for exchange of information on latest threats and vulnerabilities and mitigation strategies to cyber-attacks.

7. NOTABLE INCIDENTS OF CYBER WARFARE:

1988: Solar Sunrise

In the year 1988, a worm, intended to be an experiment, led to computer repairs of US$100 million. This gave birth to current day's DDoS attacks. Robert Tappan Morris created the experimental worm at Cornell University, USA. The worm is popularly known as the Morris worm, deriving its name from its creator. Three teenagers in 1998 actively hacked up to 500 computers in the US; the computers included government systems as well. The attack affected the nation's IT infrastructure to a very large extent. This cyber warfare is popularly known as the case of Solar Sunrise. The name is derived from the fact that Sun Solaris was the common operating system in all hacked computers.

2010: STUXNET

A malicious worm known as Stuxnet was spotted in 2010.This worm was responsible for destroying Iran's nuclear power. It allows the automation of electromechanical processes and it is used to resist the machine resources. Stuxnet design is in such a way that it is used for hacking modern supervisory control and data acquisition. Siemens released a detection and removal tool for Stuxnet that recommends contacting customer support if a worm is uncovered. It also advises installing Microsoft updates for security and stopping the use of third parties.[8]

2014: The Sony Corporation Attack

This attack took place in October 2014; its motive was to take revenge. The computer systems of Sony Corporation were hacked and the attackers stole a huge amount of private data from the Hollywood Studio, displayed them every week, and exposed it in every field from journalists to potential cyber criminals.

2017: WannaCry

WannaCry ransomware attack took place in May 2017 and is considered, as the worldwide cyber-attack. Its aim was to target computers running Microsoft Windows Operating System and encrypting information and asking for ransom payments in the form of Bitcoin Cryptocurrency. It entered older Windows system through Eternal Blue and the misuse was uncovered by the United States National Security Agency (NSA). Few days before the attack Eternal Blue was robbed and leaked by a group called The Shadow Brokers. While the Microsoft have released some patch to slow down the misuse, much of the spread was from organizations that were using the older version of Windows. Wanna Cry took benefit by installing entrances onto infected systems. The attack was expected to have affected over 200,000 computers across 150 countries, with a loss ranging from hundreds of millions to billions of dollars.[9]

8. CONCLUSION:

In today's modern era, technology and communication has been developed in large-scale but these technologies have also given rise to sophisticated criminal activities like online fraud, Cyber stalking, Cyber bullying etc. Most governments have cyber security agencies (cyber army) to assist protect against cyber attacks that may occur during a cyber war, the militaries hire computer and security professionals to assist in defence and, if necessary, attack of other countries. Cyber security is not the responsibility of an individual or an organization, but of the country has a whole. To conclude, the ever growing cyber warfare technologies are used for both good and bad motives. With the anti-cyber warfare technologies, it can be expected that there may be solid solutions to deal with cyber warfare techniques used for ill motives.

REFERENCES:

[1] https://en.m.wikipedia.org/wiki/Cyberwarfare

[2] https://www.techtarget.com/searchsecurity/definition/cyberwarfare

[3] https://www.britannica.com/topic/cybercrime

[4] https://nios.ac.in/media/documents/Military_Studies_374/Book-2/Chapter-15.pdf

[5] https://www.analyticssteps.com/blogs/cyber-warfare-all-you-need-know-about-it

[6] https://www.orfonline.org/expert-speak/india-crucial-cyberwarfare-capabilities-need-to-be-upgraded/?amp

[7] https://www.imperva.com/learn/application-security/cyber-warfare/

[8] https://www.ijert.org/research/study-on-cyber-warfare-during-2001-2019-IJERTCONV8IS05041.pdf

[9] https://www.kaspersky.co.in/resource-center/threats/ransomware-wannacry