The War of Information Age: Cyber War

Harsh Wadhwani

Rajiv Gandhi National Cyber Law Center, National Law Institute University,
Bhopal, 462044, Madhya Pradesh, India

Abstract

The age in which we are living is known as the information age, because in today's world everything is Internet of Things and hence life has become easy but information depended, previous war which took place affect human lives directly but in this generation if one wants to hurt human lives they do not need arms and ammunition to do so but they can do it using computers, by making misuse of computers which give rise to cyber crimes and when one or many cyber crimes comes together which similar to when arms and ammunition comes together against any body gave rise to a war and hence the next war is going to be an information war that is a cyber war.

Keywords: *Computer, Cyber Crimes, Cyber Security, Information Internet, War.*

1. Introduction

People have addiction towards computers and internet and hence rather than storing there documents in files and folders in physical medium they believe in storing them in digital medium in their computers and hence it saves there money, time and space accept this people are getting more dependency on Internet of Things, i.e. everything is based on Internet from there computers to mobiles to air conditioners everything and hence they feel that life is easy with growth of technology, but that's not true with ease in life problem also comes and hence security issue arise here, as all these things comes under an umbrella term, i.e. cyber space and hence it is a matter of cyber security.

How this information war will take place now, as every sensitive critical information is in this cyber space, affecting human lives becomes more easy as limitation of boundaries are over, there are no boundaries between any country now and hence cyber crimes can be easily committed on just one click in one country and this may affect different parts of the world at one time, if we compare a cyber war and a physical war, the former can produce more loss as compared to latter by attacking at one time on so many different places together, cyber war is something which requires some computers, knowledge of, how to breach the cyber security and how to commit cyber crimes and getting into state of a war.There are different cyber crimes which committed together or individually can form a cyber war and having a proper cyber defense for it is a difficult thing but still some major safeguards should be taken in order to protect the cyber space and hence form a kind of preparedness toward this war.

2. Way to Cyber War

To affect public at large one need to have proper requirements and strategy to form a cyber war, this can be easily achieved by use of some dangerous cyber crimes which directly or indirectly affects lives of people and hence disable them from use of daily access and services and, this can be done by denying access of them to services provided to them which is used by them regularly, to take away the charge of websites of critical infrastructure like, banks, etc. Other attacks such as use of botnets to convert computers into zombies, also one can use crypto locker to lock someone's system and then demand for extortion, these are few ways by which one may get whole world into cyber war and these ways are further discussed in details as,[1]

2.1 Denial of Service and Distributed Denial of service

Denial of service attack as the name says it denies services of people, it may be any website and hence slow downs the network, totally interrupt the services of a system, attacker sends many bogus request to a system at single time and hence leads to DOS, due to overload of request it may sometimes crashes the server and hence is a lethal attack to affect the system. Another one is Distributed denial of service, this attack attempts are made to make a single machine unavailable of resources by using different computer systems to send request on it leading to denial of service, nature of both is same just number of computer in one is more and in one is less.[2]

2.2 Website Defacement

This is a cyber crime committed by attacker to take the full charge of website and can do anything with it, i.e. can change its appearance, to change the web host, to change the content of the website and by doing such activities to mislead and deceive people and hence giving lives of people in danger.

2.3 Use of Botnet (Zombie Army)

Botnet also known as bots or a zombie army is nothing but internet computers which are used by attackers and the owner are unaware of it that there computer is used by attacker to forward spam mails, viruses to other computer using internet and botnet is one of the main issues when we talk about internet of things, the name zombie comes here because bots enters into computer and make use of someone else computer according to them and can cause any harm and hence known as zombie.

2.4 Crypto-Locker

A crypto-locker is a malware which comes in form of a attachment of e-mail and when the user opens it, affects the computer and locks the system giving a pop up to pay the ransome if the user wants it computer to get decrypted and hence it is a new one in this time and lethal too.

These are some attacks which may result to the cyber crimes discussed above which are more than sufficient to lead to a cyber war and in this combatting it is a difficult thing still if some basic preparedness method used can lead to a protection of computers and cyber war may be avoided but that is not sure.

3. Protection against Cyber War: Is It Possible?

Cyber war, is a kind of war and hence providing absolute cyber security is not possible, as it is said that there is nothing called absolute security, but still there are some preventive methods which if implemented with proper due diligence may lead to some protection or at least before such situation arises one may get alert of it, those measures are,

3.1 Use of Firewall

What is a protected network? It is something which uses devices with due diligence in order to make a network secure from outside network, i.e. use of Firewalls which controls incoming outgoing network traffic by implementing firewall rules this helps in creating a secure internal as well as external network they are of two types, they are packet filter firewalls, which blocks the packets whose packet address are defined in firewall rules to be blocked at network level and application layer firewall this works on application layer and intercepts all packets at application from another and is much safer.[3]

3.2 IDS & IPS

Intrusion detection system and Intrusion prevention system is another devices are used in which IDS provides network with level of preventive security and generates alarms when there is detection of some intrusion they are host based IDS and network based IDS, former works at host level at individual computer level the latter works at network level that is group of computers and computer networks, next comes IPS which controls access to IT network and protect systems from attack and hence its work is to take action and block the intrusion.

3.3 Demilitarized Zone

Formation of DMZ i.e. demilitarized zone is to make a zone between outside network and private network by using firewalls, it can be a single firewall DMZ in which one firewall is used and rules are set accordingly or dual firewall DMZ, which is formed using double firewall and hence form a more secure DMZ and protects network.

These are the following ways to protect a computer and computer system but do these methods really protect a computer system or network, yes and no both, it gives a idea that a cyber war may take place, which fulfills the saying that prevention is better than cure, but at times no as it does not protecting our computers or networks as the attacker may have some lethal attacks to compromise them which lead to zero day attacks and hence there is no absolute security from cyber war.[4]

4. Conclusions

There can be more attacks, cyber crimes which are coming day to day and destroying many computers and creating a situation of cyber war, also with that preparedness will also come and hence cyber war is something which do not have a perfect method to be fought this is subject to matter of time and will grow with time and use of technology in proper way will give a way out to combat and achieve win in it.

Acknowledgments

I would like to express my deep gratitude towards my parents Dr J.L. Wadhwani and Shalini Wadhwani to inspire me to right this paper and also to my Professor Dr Atul Kumar Pandey for guiding me in topics related with cyber space and cyber security and helped me to understand basics of subject so I was able to write this paper, I thank Every near and dear one to be a support while writing this paper.

References

[1] Fred Schreier. (2015). On Cyberwarfare. DCAF HORIZON 2015 WORKING PAPER No. 7.

[2] BEHROUZ A. FOROUZAN (2013). Data communication and networking. 5th ed. New York: Tata Mc Graw Hill Education. pg1079-1079.

[3] Nina Godbole (2012). Information Systems Security. New Delhi: Wiley.

[4] War games in the fifth domain, dipl-Ing(FH) Karin kosina masters thesis.