CYBER WARFARE IN TODAY'S INFORMATION AGE

PRATHIKSHA A R

M-Tech in Cyber Forensics and Information Security,

Department of Information Science & Engineering

New Horizon college of Engineering, Bangalore- 560103

Abstract- In today world, the internet has become very important part of our day-to-day life. Anyway, these days the cyber warfare is one of the overused terms. Cyber warfare is also poorly defined. Cyber warfare helps in inflicting maximum damage to the opponents. Nowadays, due to globalization it has become very easy to gather and receive information's and sensitive data about everyone and everything. The purpose of this research paper is to explain all the basic concepts of the Cyber warfare (CW), it's tactics, tools, motivations and its most common Cyber Attacks.

Keywords: Cyber warfare, cyber tools, motivations, Cyber Attacks.

INTRODUCTION

The time we are living in is also called as the Information Age as today's information is worth more than any other commodities. Proper use of the internet will make our daily life simpler, easier and faster. There are many benefits of internet but it all depends on how individual utilizes it. However, now a days the cyberspace has

Increased drastically as powerful competition in open-warfare.

These days you don't have to travel distances to fight a war, there's no need to spend hours-and-hours to reach the target. Within seconds or even micro seconds you can target from anywhere in this globe. Cyber space can be used to steal an individual's sensitive information or data.

Fear can be induced among people in many forms by using cyber warfare. On a daily basis many nations register cyber-attacks in every minute.

All the devices that we are using on a daily basis that are connected via internet can be vulnerable and can cause major damage to an individual or a nation.

So, does that mean it is serious?
-Absolutely, it can be highly serious.
What can be done about this?

- Take all the basic precautions to secure your sensitive data.
- Avoid sharing personal details and information online.
- Make sure people that you are communicating with are from a trusted and secured source.

In today's data cantered world the greatest challenge that we face is cyber warfare as all our information are easily accessible over the internet.

Cyber warfare will be an invisible war field, where different hackers from various countries will come together for warfare purpose.

Motivations of Cyber warfare:

There are many reasons for a country to undertake offensive cyber operations.

- Military:
  Cyber has become a potential threat for the country's security. So, this has become the interest for the militaries to declare war among several nations.

- Civil:
  Civil is the potential targets of the internet for the variety of the data transmission and collection medium.

Other motivation includes hacktivism, income generation, private sector, non-profit research.

Categories of Warfare:

- Espionage
- Surprise cyber attack
- Propaganda
- Sabotage
- Economic disruption

Most common attacks on Cyber Warfare:

- DDoS (Distributed denial-of-service)
- The love bug Sobig, Bagle and My Doom
- The rise of Botnets

Examples of some of the cyber warfare attacks:

Example 1: "STUXNET"

In the year 2010, "STUXNET" the computer virus demolished a nuclear weapons plant in Iran.

Stuxnet is different from others because it caused kinetic damage in the real-world. Stuxnet just began spreading on windows machine throughout the globe. Simultaneously it was searching for PLCs (Small computers which control things like factories, like the power grid).

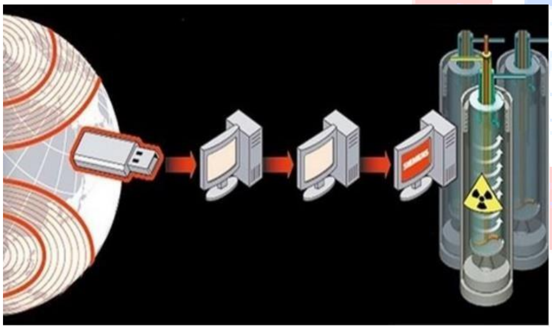
The code is put onto the PLCs and this is normal process code goes onto the PLC which turns the PLC on or off and controls it. These codes were in zeros and ones which was targeting the uranium plant in Iran. Uranium plant in Iran is a very secured place that you can't connect it through internet. So, the only way to get into the plant was by a USB key. Without knowing about this someone would take this USB key with them and plug it inside a computer which would affect the entire system.

A country can develop a cyber weapon without any complications as it is very easy and cost effective. A power grid can be easily shut down using a cyber weapon. By doing this electricity will be cut down and this would cause a serious effect on everyone.

They can't even withdraw money from ATM's as they are not working. Water waste and treatment plants will stop working due to which there will be no clean

water. Stores potentially aren't even operating. Your credit cards will also not work on stores. There will be absolutely mass panic among people.

Even military operations can be disabled by shutting down the computer network and GPS of the system because of this it's functionality will be lost. It will take many days to recover the backup and bring the system ready for execution. This can cause tremendous damage. The opponent are capable of completely blind siding your armies, air force and your nations military source by shutting down their cyber systems. This will be a serious and major damage to the country.



Example 2: "KUDANKAULAM NUCLEAR POWER PLANT"

Kundankaulam nuclear power plant is considered as one of the biggest single nuclear power stations present in India. The plant is situated exactly in the district of Tamil Nadu.

After one week of that attack officials confirm cyber-attacks on this. This hack was similar to the hack which was made by Lazarus Group of North Korea.

Cyber security strategy:

A cyber security strategy is the high-level planning about how your organization will be able to protect or secure its assets forthe time period of next 3 or 5 years.

Some cybersecurity measures:

- Implement good networksegmentation, if it is implemented properly these strategies will make it very difficult for the adversary to gain access to our sensitive details or information or to locate it.
- Apply the firewall, earlier the network segmentation was implemented with the help of firewalls at the organisation's internet gateway.
- Use the VPN (virtual private network) as the remote access method.
- Only use the strong passwords to keep your sensitive information and systems to be protected.
- Keep an awareness about vulnerabilities and implement good patches and the updates.
- Activate policies on your mobile devices.
- Provide cybersecurity awareness and training program for every employee.
- Implement cyber security detection and

incident response or action plans.

- Always keep in mind to never allow any machines with are on the control network to make direct interaction or to talk directly with the business network machines.

Conclusion:

Today in this information age, where today's information is worth more than any other commodities, data plays an important role for many cybercrimes and their vulnerabilities to the cybercrime. Even though all the organisation, private, companies, governments, individuals try to protect their data or sensitive information about them, due to some vulnerabilities hackers can easily get access to these information's which can be used against them. Data protection, security, privacy, networks all are interdependent. As the internet is linked up with almost all the computer, sensitive data, government computers and important infrastructure are all at risk. These consequences of cyber attack can become so great that in many developed nations the attack threat can deter political actions and even military. By seeing all this the private citizens, governments and many organisations and companies they have started to work and collaborate together for implementing active cyber defence in their nations.

References:

[1] Kostyuk, N., and Zhukov., M., Y. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution, 63(2)., 317-347

[2] Porter, Chris (n.d). CYBERSECURITY AND DETERRENCE. Retrieved from https://www.lawfareblog.com/cyber-warfare-front-line-everywhere-usgovernment-isnt P. Apps, Analysis: In cyber era, militaries scramble for new skills, Reuters, accessed 23/06/14 (February 2012).

[3] J. Marcus, Are we really facing cyberwar?, BBC News, accessed: 18/05/14 (March 2013). URL http://www.bbc.co.uk/news/technology-21653361

[4] Uk 'complacent' over military cyber-attack risk, mps warn, BBC News, accessed: 22/05/14 (January 2013). URL http://www.bbc.co.uk/news/uk-politics-20952374

[5] NATO, The tallinn manual on the international law applicable to cyber warfare, Online, accessed: 22/05/14 (March 2013). URL www.ccdcoe.org/249.html

[6] Sun Tzu, The Art of War, Shambhala Publications, 2005.

[7] J. Carr, Inside Cyber Warfare, Second Edition, O'Reilly Media Inc, 2012.

[8] R. Wilking, Expert: Us in cyberwar arms race with china, russia, NBC News, accessed 25/05/14 (February 2013). URL http://investigations.nbcnews.com/_news/013/02/20/ 17022378-expert-us-in-cyberwar-arms-race-with-china-russia

[9] A. Sharma, R. Gandhi, W. Mahoney, W. Sousan, Q. Zhu, Building a social dimensional threat model from current and historic events of cyber attacks, in: Social Computing (SocialCom), 2010 IEEE Second International Conference on, 2010, pp. 981–986. doi:10.1109/SocialCom.2010.145.