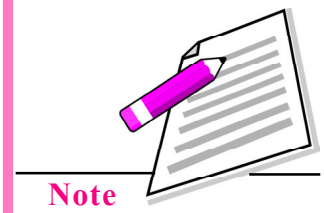


Note

15

374en15

CYBER WARFARE

In the last three lessons we have learnt about Nuclear, Biological and Chemical Warfares. With the advent of information technology and increased use of cyber space there is a new form of warfare that is being extensively used by adversaries and that is cyber warfare.

Cyber war relates to the use of computer technology to disrupt the activities of a state or organization. It is the deliberate attacking of information systems for strategic or military purposes. It implies disrupting or destroying information and communication system of an adversary, and trying to know everything about an adversary, while keeping the adversary from knowing much about oneself.

Cyber warfare involves both offensive and defensive operations pertaining to the threat of cyber attacks, for espionage and sabotage. There has been controversy over whether such activities can be called "war". Nevertheless, nations have been developing their capabilities and engaged in cyber warfare either as an aggressor or defendant, or both.

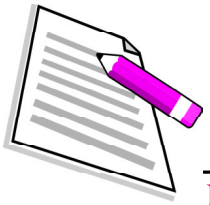
Objectives

After studying this lesson, you will be able to:

- explain the definition of Cyber Warfare;
- recognise the types of cyber threats;
- describe the types of cybercrime, cyber attackers and cyber weapons;
- explain cyber penetration and the remedial measures to be taken and
- explain the cyber security policy.

15.1 Definition of Cyber warfare

Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption". Other definitions also include non-state actors, such as terrorist groups, companies,



Note

political or ideological extremist groups, hacktivists, and transnational criminal organizations. Some governments have made it an integral part of their overall military strategy, with some having invested heavily in cyber warfare capabilities.

Cyber warfare is essentially a formalized version of penetration testing in which a government entity has established it as a warfighting capability. This capability uses the same set of penetration testing methodologies but applies them in a strategical way to

(a) Prevent cyber-attacks against critical infrastructure

(b) Reduce national vulnerability to cyber attacks

(c) Minimize damage and recovery time from cyber attacks

Offensive operations are also part of these national level strategies for officially declared wars as well as non contact war even when nations are not at war.

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

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

15.2 Types of Threat

(a) **Cyber attacks:** These are the intrusions where immediate damage or disruption caused are the main concern.

(b) **Cyber Espionage:** Cyber espionage is an act of intrusion which can provide the information needed . Traditional espionage is not an act of war, nor is cyber-espionage, 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).

(iii) The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.

(iv) The "Titan Rain" probes American defence contractors computer systems since 2003.

(v) The Office of Personnel Management data breach, in the US, widely attributed to China.

(c) **Cyber Sabotage:** Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as command and control systems could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. The civilian realm is also at risk, some potential targets include the electric power grid, trains, or the stock exchanges. Non-state actors can play as large a part in the cyberwar space as state actors, which lead to dangerous, sometimes disastrous, consequences. Small groups of highly skilled malware developers are able to as effectively impact global politics and cyber warfare as large governmental agencies.

(d) **Cyber Propaganda:** 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 behavior 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 recreist potential members.

Intext Questions 15.1

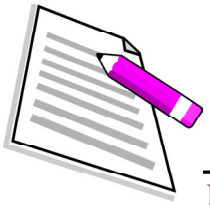
1. Fill in the blanks.
   (a) _____ is the evolution of policies and procedures to protect own information and information system.
   (b) The aim of _____is to control information and influence public opinion.
2. Define cyber warfare.
3. What is meant by Cyber Crime and Cyber Security?
4. Mention the types of cyber threats.

15.3 Cyber crime, Cyber Attackers and Cyber Weapons

15.3.1. Emergence of Cyber Crime

Let's take a look at the causes and how Cyber Crime emerges:-

(a) In this world of network centric environment there has been a phenomenal growth



Note

of internet usage; this has made our cyber space vulnerable to various crimes.

(b) Advancement in the field of electronics and technology has made common the use of sophisticated computer tools not only for us but also for our adversaries.

(c) There is a tendency where victims of cyber crimes hesitate to own upto attacks. This may be to prevent spread of rumours or damage to their reputations eg. banks etc.

(d) We are dramatically becoming more and more dependent on ecommerce and networked based solutions to optimise our resources; this in turn has made us vulnerable to cybercrime.

15.3.2 Types of Cyber Crime

In todays world there are as many cyber crimes as man's fertile and imaginative brain can think of Cybercrimes can broadly be categorised as:

(a) Fraud and Forgery: This is primarily evident in the field of commerce and economy.

(b) Damage to or Modification of Computer Data or Programme: This can be for private sector, public sector or for defence establish, such as ATC & Radar system.

(c) Unauthorised Access to Computer System and Surveillance: This is commonly seen in commercial websites, e.g., Phishing, spywares and data spoofing.

(d) Unauthorised Reproduction of Computer Programmes: These are the cases of piracy.

15.3.3 Cyber Attacker

Cyber attacker aims at causing criminal threats or to cause national security threats. Some cyber attackers are -

(a) Hacker: A computer user who intends to gain unauthorised access to a computer system.

(b) Crackers: A cracker is a hacker with criminal intent, who maliciously sabotages computers, steals information located on secure computers and cause disruption to the networks for personal or political motives.

(c) Insider: A disgruntled insider (a current or former employee) of an organisation is one of the principal sources of cybercrime. An insider's knowledge of the organisation's network often allows them to gain unrestricted access to cause damage to the information system or to steal sensitive data.

(d) Terrorist: Cyber attackers who use IT and internet to plan & execute their

Note

activities, raise funds, spread propaganda, shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of forcing or intimidating a government or civil population.

(e) **Foreign Intelligence Services:** Foreign intelligence surveillance who use cyber tools as part of their espionage tradecraft for acquiring sensitive information about their adversary.

15.3.4 Cyber Weapons

So far, you have understood what is cybercrime. But just as in all other crimes, there are certain weapons used to commit these crimes. Let us find out what they are.

(a) **Viruses and Worms:** It is very commonly heard or noticed term in our day to day computer life. These are the codes that execute within host program. Whenever anything goes wrong we don't hesitate to blame viruses for the matter. But something more complex like Worms (programs executed independently) are also used.

(b) **Trojan Horses:** These are programs that work in disguise. Trojan Horses are unauthenticated program contained in a legitimate program which performs functions unknown to the user. Likely places for Trojan Horses to attack are:-

(i) OS.

(ii) Software downloaded from internet.

(c) **Logic /Knowledge Bombs:** These are hidden functions that becomes active when triggered.

(d) **Knobots:** Also known as Knowledge Robots, they keep the processed data and keep storing the knowledge.

(e) **Adware:** Adware is a programme that can be embedded within useful programmes. These popup while using the computer they are embedded in and have a lot of nuisance value.

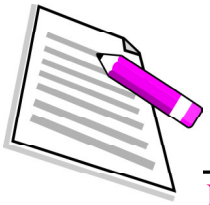
(f) **Spyware:** Spyware is also a programme that is embedded with a useful programme. However, they are generally programmed to collect information such as user's web surfing habit /preferences and e-mail. The illegal part of the activity is that all the activity occurs without the users consent.

Intext Questions 15.2

1. Fill in the blanks.

(a) Knowledge Robots are known as_____.

(b) Computer user who intends to gain unauthorised access to a computer



Note

system is a _____.

(c) A _____is a hacker with criminal intent, who maliciously sabotage computer, steal information located on secure computers.

(d) _____ are programs that work in disguise.

(e) Adware and spyware are one and the same (True/False)

2. Mention the types of cybercrime.

3. List the various types of cyber weapons.

15.4 Cyber Penetration, Remedial Measures & National Cyber Security Policy

15.5.1 Cyber Penetration : Modus Operandi

How do our adversaries operate to penetrate into our Cyber Space? They send out numerous e- mails to internet users for cyber hacking. Generally these mails have spywares which are detrimental to the host computers and result in sharing /retrieval of data stored on the hard disk. Sometimes it also leads to crashing the computer. These spywares could facilitate remote administration of the host computer.

Whenever a hacker penetrates a computer, he would attempt to install a spyware that will give him access to that computer at his will. He also may install malicious programme which would collect information from the computer and through internet, down load all files and particular IP address. An antivirus programme alone is not good enough to detect all such rogue programs, because while viruses are designed to propagate openly, spywares are designed to propagate by stealth. So the technologies required to detect viruses and spyware are also different.

15.5.2 Indications

How can I get indication that my computer is Infected? There are very apparent indications which show your computer is infected. Be vigilant and look for the following:

(a) Poor system performance.

(b) Abnormal system behaviour e.g., system restarts or hangs frequently.

(c) Unknown services are running.

(d) Crashing of applications.

(e) Change in file extensions or contents.

(f) Hard Disk is busy or its light glows continuously.

Note

15.5.3 Remedial Measures

Although you may not be able to catch the indications of your computer being infected, there are certain precautions you can observe to keep your systems safe from attack. These are -

(a) **Install Latest Patches for OS:** Install latest patches for the OS and application being used from a trusted website only. A good Firewall would act as the first line of defence to alert the user if any application / programme is trying to connect to his PC over the internet. However, a firewall has the following limitations:-

(i) It cannot protect your computer against malicious insiders i.e., spoofing attacks.

(ii) It cannot protect against connections that don't go through OS (i.e., backdoors).

(iii) It cannot protect against viruses which are e-mail borne.

(b) **Install a Good Internet Security Suite:** Nowadays various Internet security suites are available in the market. They combine the functionality of antivirus, antispyware, firewall, parental controls etc. Alternately, as a user, you must install an antivirus as well as an antispyware programme and must download latest virus signature periodically (preferably daily).

15.5 CERT and National Cyber Security Policy

The Department of Information Technology created the Indian Computer Emergency Response Team (CERT-In) in 2004 to thwart cyber-attacks in India. That year, there were 23 reported cyber security breaches. In 2011, there were 13,301. In response, the government created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defence, space and other sensitive areas. India had no cyber security policy before 2013. The government unveiled a National Cyber Security Policy 2013 on 2nd July 2013. The National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology.

The Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents. This is achieved through a combination of institutional structures, people, process, technology and cooperation. The objective of this policy is to create a secure cyberspace ecosystem and strengthen the regulatory framework.

The Computer Emergency Response Team (CERT-In) has been designated to act as

a nodal agency for coordination of crisis management efforts. CERT-In also acts as an umbrella organization for coordination actions and operationalization of sectoral CERTs.

Intext Questions 15.3

1. Expand the following-
   (a) CERT
   (b) ICT
   (c) NCIIPC
2. What are the indications of the computer system being infected?
3. What are the limitations of firewall?
4. Why is a good firewall called the first line of defence?

ACTIVITY 15.1

Watch the documentary "Zero Days" at https://topdocumentaryfilms.com/zero-days/

What You Have Learnt

This lesson in Cyber warfare has given you an insight into the following:

- Certain definitions connected with cyber warfare;
- Types of threat which include cyber espionage, cyber attack and cyber sabotage and cyber propaganda;
- You have also studied about types of Cybercrime, Cyber Attackers and Cyber Weapons
- Cyber Penetration and indication that give us an idea that our computer is infected. Remedial measures have to be under taken to prevent cyber attacks.

Terminal Exercises

1. Write short notes on
   (a) Cyberwarfare.
   (b) Cyber Espionage.
   (c) Cyber Sabotage.
   (d) CERT and National Cyber Security Policy.
   (e) Remedial measures against cyber penetration.

2. Differentiate between adware and spyware.
3. What is cyber propaganda?
4. Explain the emergence of cybercrimes and measures to check them.
5. Explain the National Cyber Security Policy.

Answers to Intext Questions

15.1

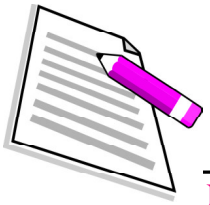
1. (a) Cyber Security.
   (b) Propaganda
2. Cyber warfare has been defined "actions by a nation-state to penetrate another nations computers or network of or the purpose of causing damage or destruction.
3. Cyber crime is committed where the use or knowledge of computer is required to cause damage.
4. (i) Cyber attacks
   (ii) Cyber espionage
   (iii) Cyber sabotage
   (iv) Cyber propaganda

15.2

1. (a) Knobots.
   (b) Hacker.
   (c) Cracker
   (d) Trojan Horses.
   (e) False
2. (i) Fraud and Forgery
   (ii) Damage to or modification of computer
3. Viruses and Worms, Trojan Horses, Logic/Knowledge Bomb, Knobots, Adware, Spyware.

15.3

1. (a) Computer Emergency Response Team (CERT)
   (b) Information and Communication Technology (ICT)



Note

(c) National Critical Information Infrastructure Protection Centre (NCIIPC)

2. (a) Poor system performance.

(b) Abnormal system behaviour e.g., system restarts or hangs frequently.

(c) Unknown services are running.

(d) Crashing of applications.

(e) Change in file extensions or contents.

(f) Hard Disk is busy or its light glows continuously.

3. (i) It cannot protect your computer against malicious insiders i.e., spoofing attacks.

(ii) It cannot protect against connections that don't go through OS (i.e., backdoors).

(iii) It cannot protect against viruses which are e-mail borne.

4. Because it alerts the user if any application/programme is trying to connect to her/his PC over the internet.