CYBER SECURITY

by

Dr. Ravi P. Agrahari

(Faculty of KSG)

Any crime that involves a computer and a network is termed as Cybercrime. It is possible when any personal computer connected to the internet.

The **Information Technology (Amendment) Act, 2008**, serves as the legal framework for tackling cybercrime in India.

Cyber security companies produce **antivirus programmes** to prevent infection from viruses and heal infected computers. Cyber security is also concerned with **developing threat-resistant firewalls, encryption and passwords** for protection against hacking and data theft.

Cyber security is not just an issue that concerns individuals and businesses but also government, since as it has national security dimensions.

Inter Departmental Information Security Task Force (ISTF)

The **Union Government** had set up an **Inter Departmental Information Security Task Force (ISTF)** with **National Security Council** as the **nodal agency to highlight the growing threat to information security in India and focus related actions.**

Considering the recommendations of the ISTF, the **following initiatives have been taken by the Government:**

1. Indian **Computer Emergency Response Team** (CERT-In) has been established to **respond to the cyber security incidents and take steps for prevention of recurrence of the same**.
2. Public key infrastructure or PKI. (a system for the creation, storage, and distribution of digital certificates which **are** used to verify that a particular **public key** belongs to a certain entity.)
3. To support implementation of Information Technology Act and promote use of Digital Signatures, **adequate infrastructure has been set up**.
4. **Research and Development activities** have been supported by GOI through premier academic and Public Sector Institutions in the country.
5. Information Security **Education and Awareness Programme** has been launched all over India.
6. **The Crisis Management Plan** was formulated in April 2010 to deal and counter cyber-attacks and cyberterrorism. It is to be implemented by all ministries and departments of central and state governments.

CYBER CHECK

It is an **advanced cyber forensics tool kit for analysing and viewing evidence files**, indigenously developed by the Centre for Development of Advanced Computing (CDAC).

Cyberterrorism

Cyberterrorism describes the acts of deliberate, **large-scale disruption of computer networks, especially personal computers connected to the Internet**. It is performed by the means of tools such as computer viruses. Some authors choose a very narrow definition, relating to **deployments, by known terrorist organisations**.

Different Forms of Cyberterrorism

1. Terrorist propaganda on the Internet
2. Privacy violation
3. Attacks on government properties

Distributed Denial of Service Attack

The **cyber terrorists may also use the method of Distributed Denial of Service (DDoS)** to overburden the computer systems and networks of governments, armed forces and businesses. **This involves sending a large number of web requests to servers, overloading them and ultimately leading to their collapse.**

CYBER WARFARE

Cyberterrorism Politically motivated hackers aiming to conduct sabotage and espionage, lead to Cyber warfare.

Cyber warfare is described as "**actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption**."

Cyber warfare can be described as "**the fifth domain of warfare**", which has become just as critical to military operations as land, sea, air, and space."

President Barack Obama, in 2009, declared America's digital infrastructure to be a "strategic national asset," and thereafter the Pentagon set up its new **U.S. Cyber Command (USCYBERCOM)** in May 2010, **to defend American military networks and attack other countries' systems**. A cyber-security and "operations centre" is also established then by United Kingdom.

Cyberwarfare Consists of Many Different Threats

1. Cyber Espionage (spy): **obtain secret information** from individuals, competitors, rivals, groups, governments and enemies to take military, political, or economic advantage.

2. Cyber Vandalism (spread negativity): This usually **involves hacking enemy websites** and defacing the web pages or **plant propaganda messages**.

3. DDoS Attack: Attempt to make a computer resource unusable by persons or groups who disrupt an Internet site or service. **In cyber warfare, DDoS (distributed denial-of-service) attacks mainly involve targeting of government and military websites.**

4. Sabotage (to break and disturb): Military activities **using computers and satellites for coordination are often at risk of equipment disruption**. **Power, water, fuel, communications, and transportation infrastructure, all of them may be vulnerable to disruption**, as they are increasingly controlled by computer systems. Particularly, **power transmission systems and telephonic systems including cell phones are susceptible to cyber warfare**. Massive power or communication outages caused by a **cyber-attack could disrupt the economy**, distract from a simultaneous military attack, or create a national crisis.

India’s Vulnerability
In recent times, cyber-attacks resemble political conflict, leading to warning from experts of the unfolding of a “**Cyber Cold War**”. It is said that massive cyber-attacks may precede future wars.

India appears to be extremely vulnerable due to huge growth in government state-wide area networks and **44 mission e-governance mode projects**, in addition to **electrical grid, cell phones, oil and gas infrastructure**. This is on top of the private industry, especially the banking and finance sector deploying huge number of online transactions.

Response
The **main agency** dedicated to defend India’s IT infrastructure is **Computer Emergency Response Team (CERT) within the Department of Information Technology**. It performs its **functions in coordination with the National Informatics Centre**, the government’s service provider.

Dedicated cyber warfare groups operate in the **Defence Intelligence Agency (DIA**) and India’s technical intelligence organisation **National Technical Research Organisation (NTRO).**

Shortcomings Exist in India’s Cyber Warfare Capabilities

1. Dedicated cyber warfare groups operate in the DIA and NTRO but these are **tasked only with offensive cyber warfare and not with defending against cyber-attacks.**

2. India spends less than $1 million (Rs. 5 crore) on offensive cyber warfare. There are a handful of experts available. On the other hand, China has an annual budget of $55 million and employs thousands of hackers. The US and some European nations are even ahead.

3. **India cannot counterattack, but various nations can**. For example, a secure operating system “Kylin”has been developed by the Chinese as an effective protection from such attacks. Not only this, **a secure microprocessor has also been developed by them**. This microprocessor, **unlike the US made chips, which most computers in India use**, is known to be hardened against external access.

4. India, in spite of being an IT-superpower, is almost **entirely dependent on external sources, be it hardware or software. Even for all antivirus programmes, network protocols and network hardware components, India depends on external sources**. Such vulnerable operating systems could lead to massive DDoS attacks.

Dr. Ravi P. Agrahari

A Long-Term Response Involves in Cyber Security

1. A **dedicated cyber security organisation**, which staffs police and armed forces personnel that can initiate **developing a strategy to protect national information infrastructure**.

2**. Increasing the cyber warfare budgets** and inducting more personnel.

3. **Setting up a national centre for coordinated response** to cyber-crime between various law-enforcement agencies, Internet Service Providers (ISPs) and high-quality researchers within the country.

4. **Carrying out extensive information security audits of government networks, and encouraging the private sector to do the same.** The idea would be to identify security gaps to determine exactly what the problem is and try to address its security requirement.

5. A software and hardware policy intended for **development of secure indigenous microprocessors and operating systems**, so that more and more computers use these and make computers in India, in general, more resistant to cyber-attacks.

Dr. Ravi P. Agrahari

Blockchain

Blockchain is an **online ledger of digitally recorded transactions**, which is encrypted in the form of blocks, each of which is connected by a network of computers.

Blockchain enables two entities that do not know each other to agree that something is true without the need of a third party.

As opposed to writing entries on a single sheet of paper, a **blockchain is a distributed database that takes a number of inputs and places them into a block. Each block is then 'chained' to the next block using a cryptographic signature**.

This allows blockchains to be used as a ledger, which is accessible by anyone with permission to do so. If everyone in the process is pre-selected, the ledger is termed 'permissioned'. If the process is open to the whole world, the ledger is called 'un-permissioned'.

Benefits of Blockchain Technology

A blockchain is anonymous, and hence protects the identities of the users. This makes blockchain a more secure way to carry out transactions. The algorithm used in blockchain reduces the dependence on people to verify the transactions.

1. As a public ledger system, blockchain records and validate each and every transaction made, which makes it secure and reliable.
2. All the transactions made are authorized by miners, which makes the transactions immutable and prevent it from the threat of hacking.
3. Blockchain technology discards the need of any third-party or central authority for peer-to-peer transactions.
4. It allows decentralization of the technology.

Possibilities of blockchain are:

- Confidential communication of cryptocurrency.
- Safe, cost effective and fast bank transactions.
- Secure legal documents, health data, notaries and personal documents.
- Distribution of land records and government financial assistance.
- Cloud storage, digital identification, smart communication and digital voting.

National Informatics Centre (NIC) has set up a Centre of Excellence (CoE) in *Blockchain Technology* in Bengaluru, which will provide Blockchain as a service and allow stakeholders to benefit from shared learning, experiences and resources.

The **West Bengal government** is preparing for introduction of blockchain technology for safeguarding its documents from cyber attacks. The state government’s planned Cyber Security Centre of Excellence would be assigned in executing the new ‘blockchain’ system at various departments.

Note: The Tech Mahindra and the Government of Telangana have signed an accord for establishing a country’s first Blockchain district in Hyderabad, a first of its kind Centre of Excellence for Blockchain.

Thank you