GALGOTIAS UNIVERSITY

# School of Computing Science and Engineering

Program: M.Sc

Course Code:MSCS 2310

Course Name:Cyber Security

# Course Outcomes :

| CO NUMBER | TITLE |
|---|---|
| MSCS2310_CO1 | Knowledge of cyber security principles used to manage risks related to the use, Processing, storage and transmission of information or data. |
| MSCS2310_CO2 | Implementation of Cryptographic Techniques. |
| MSCS2310_CO3 | Apply the authentication methods and prevent cyber crime |
| MSCS2310_CO4 | Apply the procedures and algorithms to stop cyber Attacks and Threats. |
| MSCS2310_CO5 | Understand the various cyber security policies and how to apply them. |
| MSCS2310_CO6 | Understand the latest trends and advances of cyber security |

# Course Prerequisites

Cryptography and Network Security

**Syllabus**

**UNIT I Introduction** **9 hour**

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

**UNIT II Cryptographic Techniques** **9 hours**

Symmetric key cryptographic techniques: Introduction to Stream cipher – Block cipher: DES – AES- IDEA. Asymmetric key cryptographic techniques: principles – RSA – ElGamal - Elliptic Curve cryptography – Key distribution and Key exchange protocols.

**UNIT III Authentication and Cybercrime** **9 hours**

Hash functions – Secure Hash Algorithm (SHA) Message Authentication – Message Authentication Code (MAC) – Digital Signature Algorithm: RSA &ElGamal based Classification of cybercrimes – planning of attacks – social engineering: Human based – Computer based – Cyberstalking – Cybercafe and Cybercrimes

**UNIT IV Cyber Threats, Attacks and Prevention** **9 hours**

Phishing – Password cracking – Keyloggers and Spywares – DoS and DDoS attacks – SQL Injection. Identity Theft (ID) : Types of identity theft – Techniques of ID theft.

**UNIT V Cyber Security Policies and Practices** **9 hours**

What security policies are – determining the policy needs – writing security policies – Internet and email security policies – Compliance and Enforcement of policies- Review.

**Unit VI Research** **9 hours**

The advances and the latest trends in the course as well as the latest applications of the areas covered in the course.
The latest research conducted in the areas covered in the course.
Discussion of some latest papers published in IEEE transactions and ACM transactions, Web of Science and SCOPUS indexed journals as well as high impact factor conferences as well as symposiums.
Discussion on some of the latest products available in the market based on the areas covered in the course and patents filed in the areas covered.

# Recommended Books

1. Charles P. P fleeger, Shari Lawerance P fleeger, "Analysing Computer Security", Pearson Education India.
2. V.K.Pachghare, "Cryptography and information Security", PHI Learning Private Limited, Delhi India.
3. Sarika Gupta & Gaurav Gupta, Information Security and Cyber Laws, Khanna Publishing House
4. Anshul Kaushik, Cyber Security, Khanna Publishing House

# Lecture1

What is “cybersecurity?”

**Some Definitions**

**cybersecurity**: “The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.”

## Some Definitions

**According to S. 1901 "Cybersecurity Research and Education Act of 2002":**

**cybersecurity**: "information assurance, including scientific, technical, management, or any other relevant disciplines required to ensure computer and network security, including, but not limited to, a discipline related to the following functions:

(A) Secure System and network administration and operations.

(B) Systems security engineering.

(C) Information assurance systems and product acquisition.

(D) Cryptography.

(E) Threat and vulnerability assessment, including risk management.

(F) Web security.

(G) Operations of computer emergency response teams.

(H) Cybersecurity training, education, and management.

(I) Computer forensics.

(J) Defensive information operations.

# Lecture1

**According to S. 1900 "Cyberterrorism Preparedness Act of 2002 ":**

**cybersecurity**: "information assurance, including information security, information technology disaster recovery, and information privacy."

One way to think about it

**cybersecurity** = security of cyberspace

information systems and networks

One way to think about it

**cybersecurity** = security of information systems and networks

One way to think about it

**cybersecurity** = security of information systems and networks

+ with the goal of protecting operations and assets

One way to think about it

**cybersecurity** = security of information systems and networks with the goal of protecting operations and assets

One way to think about it

**cybersecurity** = security of information systems and networks with the goal of protecting operations and assets

security in the face of attacks, accidents and failures

In Context

**Corporate cybersecurity** = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting a corporation's operations and assets

**National cybersecurity** = availability, integrity and secrecy of the information systems and networks in the face of attacks, accidents and failures with the goal of protecting a nation's operations and assets

Cybersecurity as a Discipline

**How to achieve cybersecurity "success"?**

**How to overcome the cybersecurity problem?**

**Must understand four factors that play into the cybersecurity equation:**

- Technology
- Economics (of stakeholders and incentives)
- Social Influences (e.g. Big Brother fears)
- Public Policy

# Lecture 2

## UNIT-1 OBJECTIVES

**After studying this module you will be able to :**

- ✓Introduce the fundamentals of cyber security
- ✓Present aboutcyberspace, importance of Cyber Security

# Lecture 2

## INTERNET GOVERNANCE-CHALLENGES AND CONTRAINTS

What will we cover today?
What is Internet governance?
Why do we need it?
What is the multistakeholder model?
What are the key arguments and dilemmas?
Why should you get involved?
How can you get involved?

# Lecture2

**Internet Governance** is the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

# Lecture 2

Internet governance should not be confused with e-governance, which refers to governments' use of technology to carry out their governing duties.

Internet governance by the idea of three "layers" of governance:

- Physical infrastructure layer (through which information travels)
- Code or logical layer (controls the infrastructure)
- Content layer (contains the information signaled through the network)

The History "[the Internet] is inherently extra-national, inherently antisovereign and your [states'] sovereignty cannot apply to us. We've got to figure things out ourselves." John Perry Barlow, 1996

Things have changed…

# Lecture 2

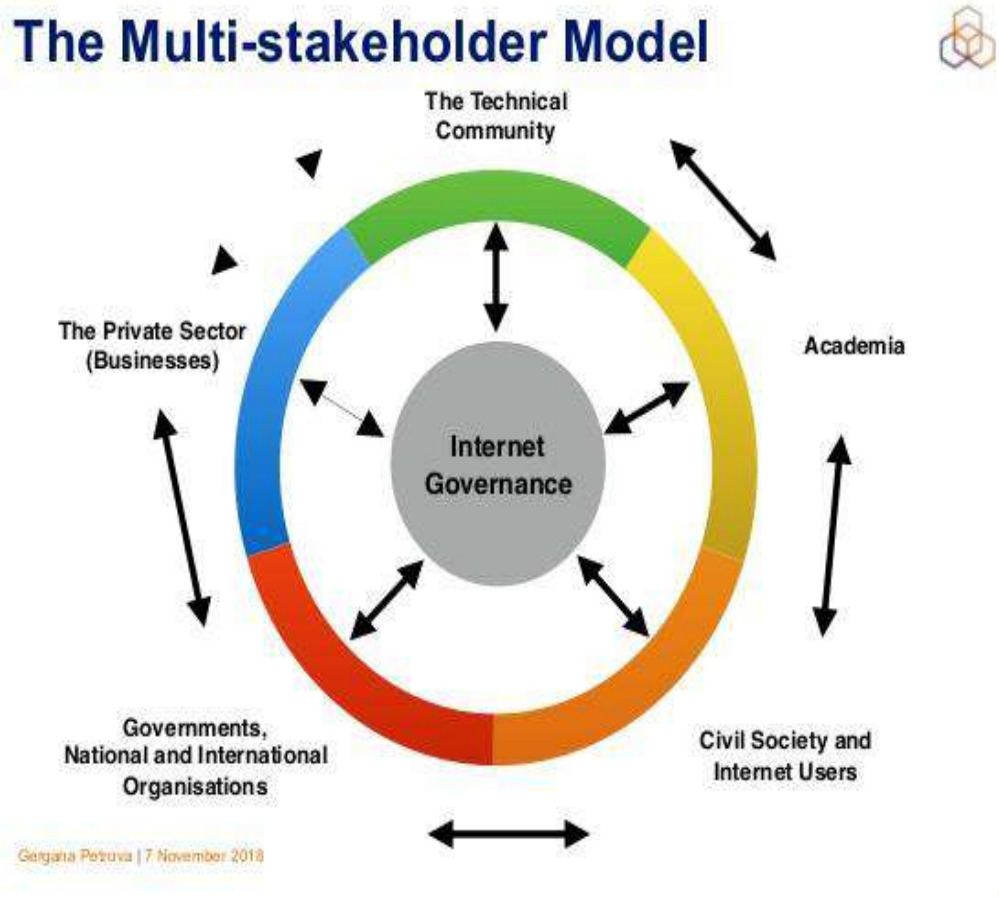
## SELF REGULATION

- Social norms worked well in the beginning of the Internet
- Self-regulation still works in a group with strong community ties, by applying peer pressure or exclusion (e.g. Wikipedia)
- ISPs try to self-regulate by imposing standards of behaviour for their customers
- Should ISPs make decisions in lieu of legal authorities? Should they judge what is acceptable content?
- Self-regulation doesn't always work, e.g. IoT market.

# Lecture 2

Definitions "Internet governance (IG) is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." World Summit on the Information Society (WSIS), 2005

# Lecture 2




Take the Poll! Go to www.menti.com and use the code 58 14 25 Which stakeholder group do you (mostly) identify with? Technical community Academia Governments / international organisations Civil society Private sector

# Lecture 2

Take the Poll! Go to www.menti.com and use the code 58 14 25 Which stakeholder group do you (mostly) identify with?

- Technical community
- Academia
- Governments / international organisations
- Civil society
- Private sector

# Lecture 3

## UNIT-1 OBJECTIVES

**After studying this module you will be able to :**

- ✓ Introduce the fundamentals of cyber security
- ✓ Present aboutcyberspace, importance of Cyber Security

# Lecture 3

# CONSTRAINTS AND CHALLENGES

# Lecture 3

## Working Group on Internet Governance

- "Internet governance is the development and applica4on by Governments, the private sector and civil society, in their respec4ve roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolu4on and use of the Internet."
- Demonstrates inclusivity
- Constructively ambiguous?
- Substantiated by the WSIS process

# Lecture 3

## Governance OF the Internet

- Better defined as Internet administration (IA)
- Largely separate from governance ON the Internet
- Actors are telcos, IETF, ISOC,RIRs, ICANN
- Decentralized functions, cooperative relationships
- Administration requires skill, engineering talent, discipline to keep complex system running

# Lecture 3

## Governance ON the Internet

- Governance of issues pre-dating the Internet
- Issue is not new, but Internet causes significant qualitative or quantitative change – Institutions exist but may not be ready – Legal structure may not be ready – People and their expectations may not be ready
- Malefactors quick to identify such gaps – Extra-legal activities quick to exploit them

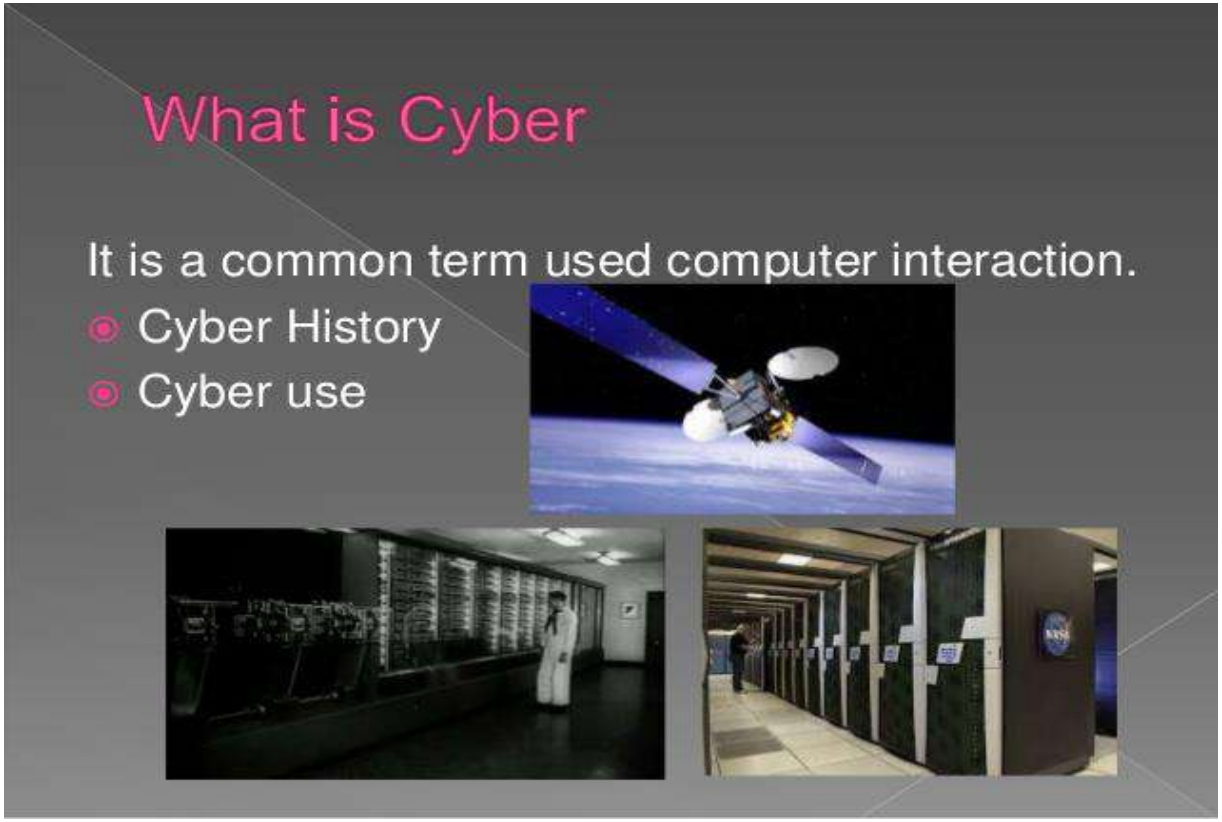
# Lecture 4

## CYBER THREATS

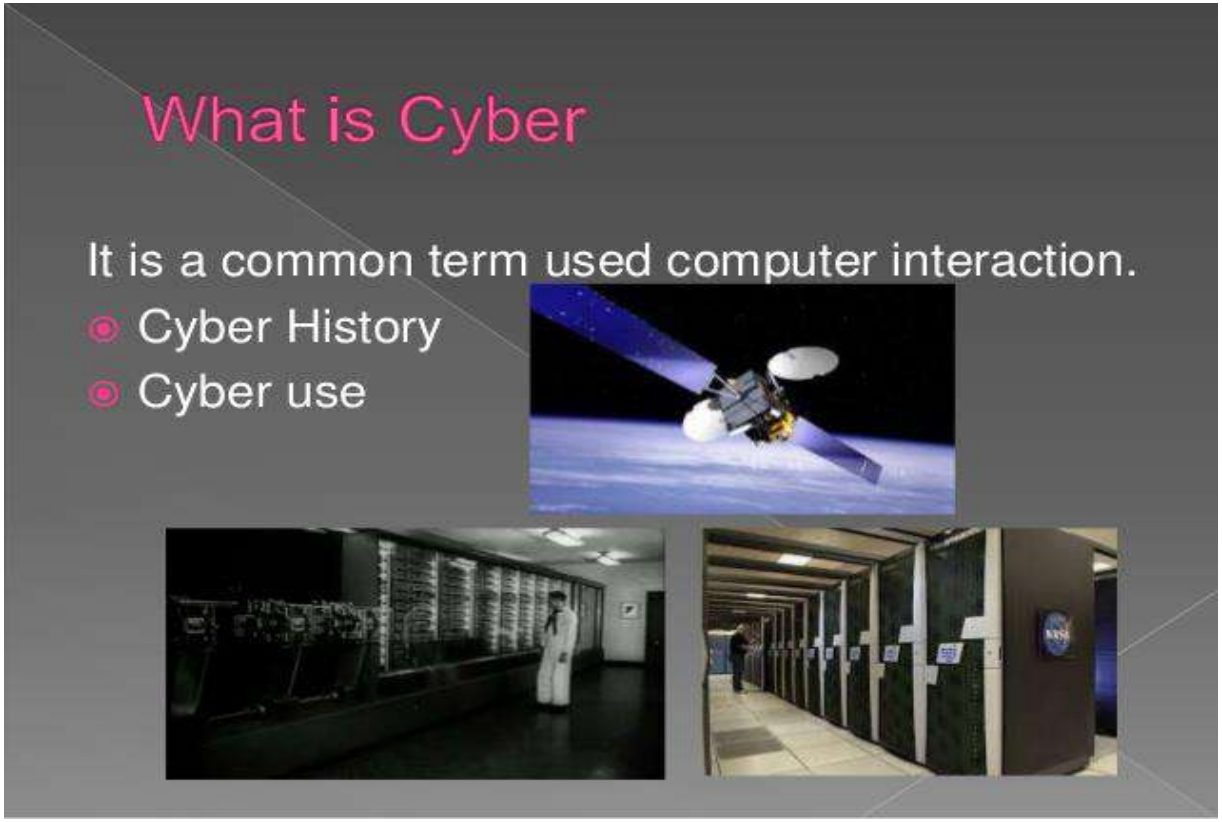
What we will cover in this?
-Cyber Warfare
-Cyber Crime
-Cyber terrorism
-Cyber Espionage

# Lecture 4

# Lecture 4


What is Cyber
It is a common term used computer interaction.
Cyber History
Cyber use

# Lecture 4


What is Cyber
It is a common term used computer interaction.
Cyber History
Cyber use

# Lecture 4


What is Cyber warfare
It is politically motivated hacking to gain control over systems and to spy.

# Lecture 4

## Timeline of cyber warfare

- 1998- The Morris worm
- 2003 – Titan Rain
- Dec,2006- Nasa (US Space launch leaked)
- April,2007- Estonian Government networks

# Lecture 4


June,2007- US Secretary of Defense account
October,2007-China's Ministry of State Security
Summer,2008- Databases of presedential Campaigns
YOU HAVE BEEN HACKED !

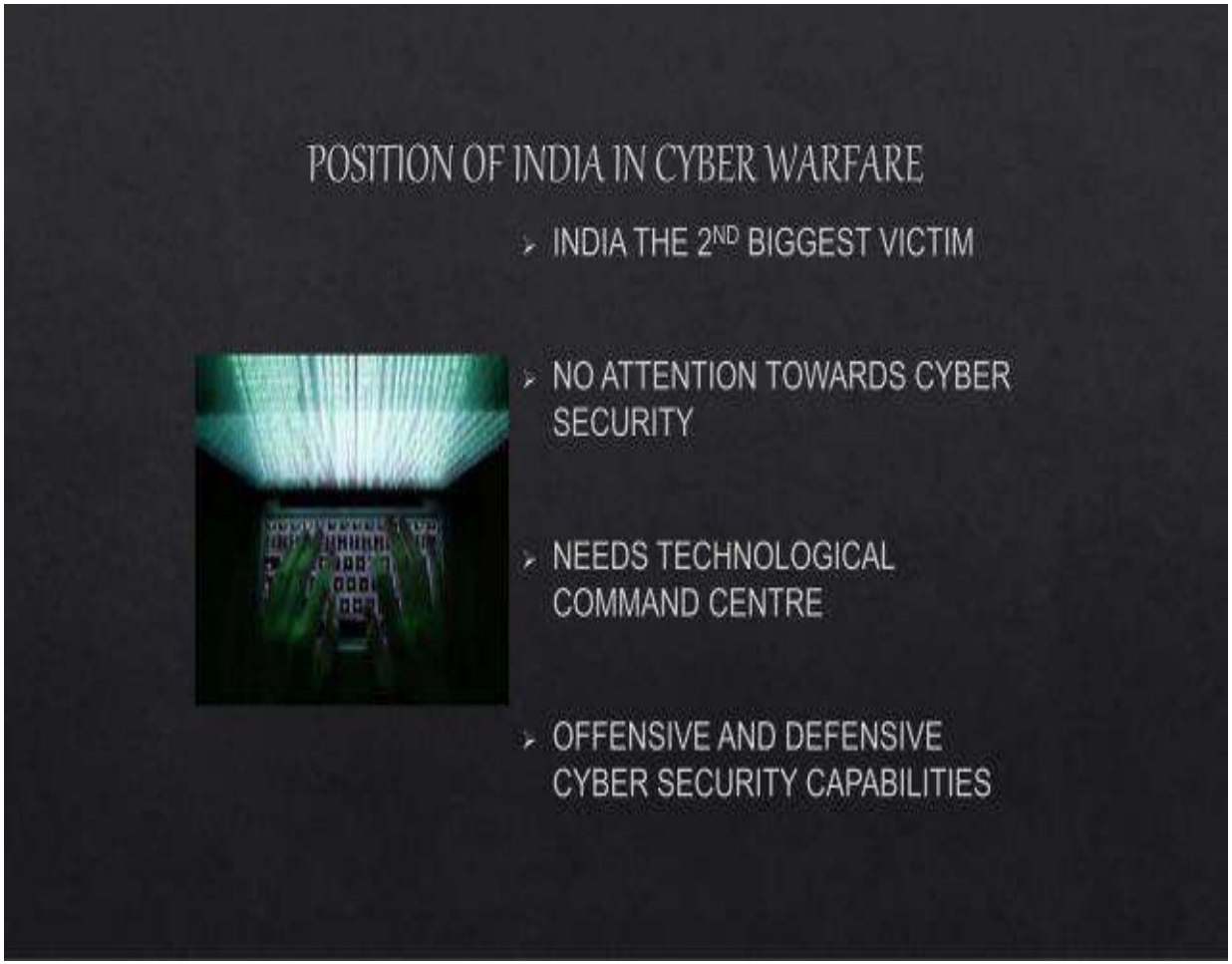
# Lecture 4

- August,2008-Computer Networks in Georgia
- January,2009-Israel's internet infrastructure
- January,2010-Iranian cyber army
- October,2010-STUXNET,Malware

# Lecture 4

- January,2011-Canadian Govt.
- July,2011-US Deputy Secretary
- October,2012-RED October
- March,2013-South Korean Financial Institutions

# Lecture 4


POSITION OF INDIA IN CYBER WARFARE
INDIA THE 2ND BIGGEST VICTIM
NO ATTENTION TOWARDS CYBER SECURITY
NEEDS TECHNOLOGICAL COMMAND CENTRE
OFFENSIVE AND DEFENSIVE CYBER SECURITY CAPABILITIES

# Lecture 4


Cyber War
LACKOF HARMONISATION
CYBER WARFARE POLICY
ROLE OF INDIAN GOVERNMENT
DIFFICULTY IN TRACING ATTACKS
THREATS FROM NEIGHNOPURING COUNTRIES

# Lecture 4

## Tips to prevent Cyber Wars :

1. **Use Strong Passwords :**
   Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

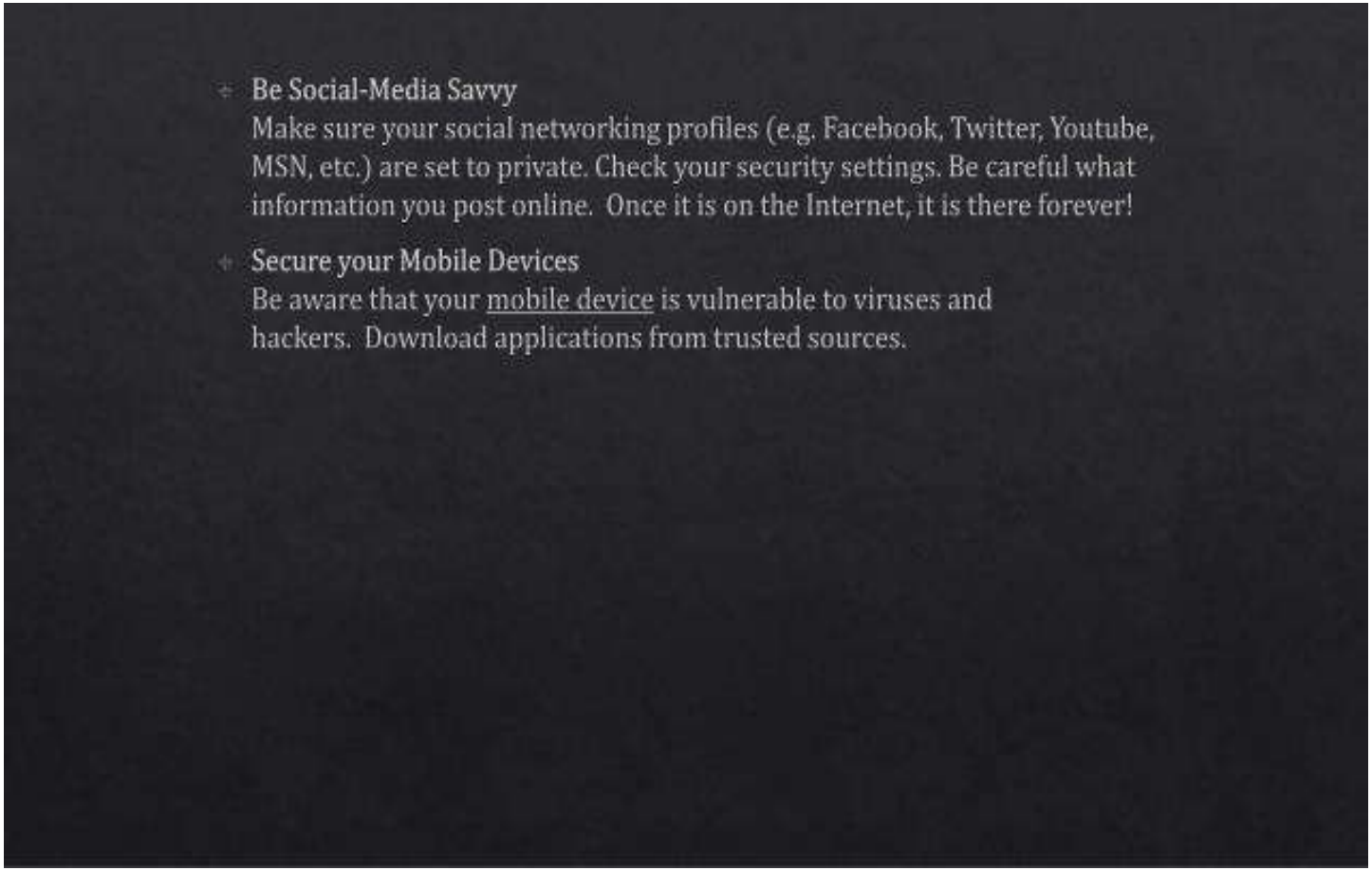
2. **Secure your computer :**

Activate your firewall:
Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

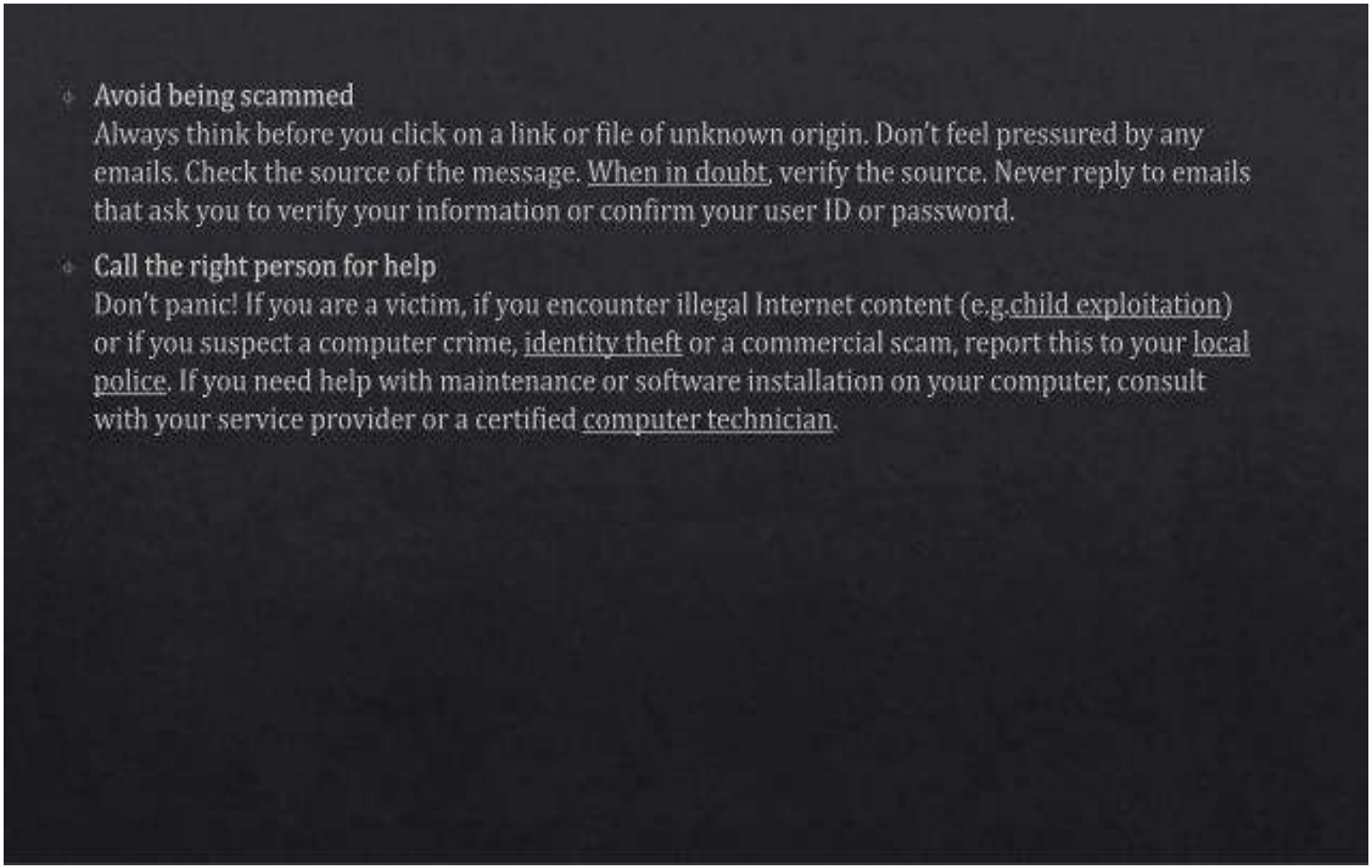
Use anti-virus/malware software:
Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

Block spyware attacks:
Prevent spyware from infiltrating your computer by installing and updating anti-spyware software

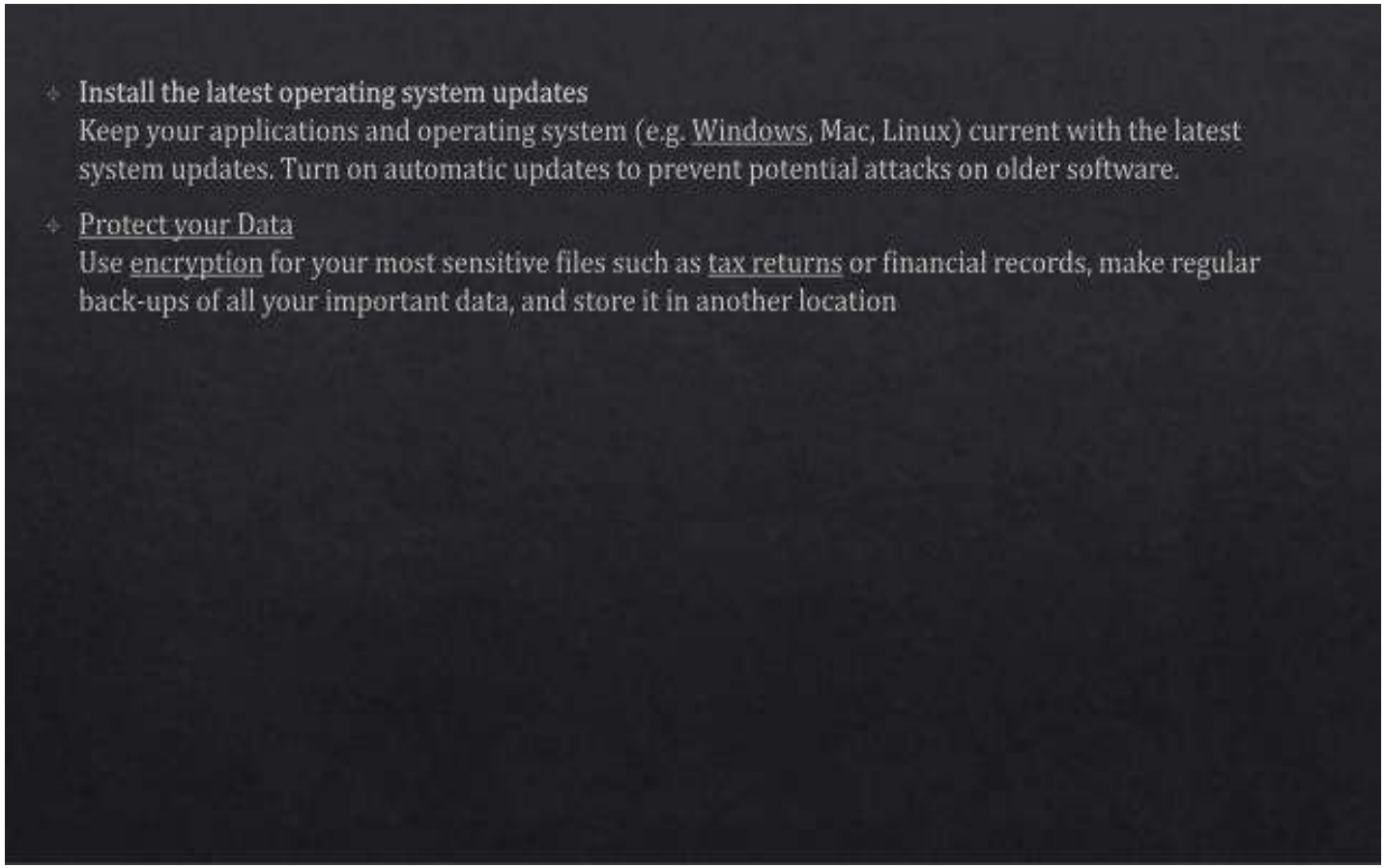
# Lecture 4


Be Social-Media Savvy
Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
Secure your Mobile Devices
Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

# Lecture 4


Avoid being scammed
Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.
Call the right person for help
Don't panic! If you are a victim, if you encounter illegal Internet content (e.g.child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

# Lecture 4


Install the latest operating system updates
Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.
Protect your Data
Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location

# Lecture 5

## CYBER THREATS

What we will cover in this?
-Cyber Crime
-Cyber terrorism
-Cyber Espionage

## Lecture 7

# CYBER CRIME

# Lecture 7

What is cyber crime?

The former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime.

Other forms include "digital", "electronic", "virtual" ,"IT", "high-tech" and technology-enabled" crime .

# Lecture 7

## History

The first recorded cyber crime was recorded in the year 1820.

The first spam email took place in 1978 when it was sent over the Arpanet.

The first Virus was installed on an Apple

Computer in 1982.

# Lecture 7

Cyber crimes includes

- Illegal access
- Illegal Interception
- System Interference
- Data Interference
- Misuse of devices
- Fraud

# Lecture 7

## Advantage of cyber security

- It will defend from hacks and virus.
- The application of cyber security used in our PC needs update every week.
- The security developers will update their database every week once. Hence the new virus also deleted.

# Lecture 7

## Safety tips …

- Use antivirus software
- Insert firewalls , pop up blocker
- Uninstall unnecessary software
- Maintain backup
- Check security settings
- Use secure connection
- Open attachments carefully
- Use strong passwords , don’t give personal information unless required

Lecture 7

# CYBERTERRORISM

# Lecture 7

- Cyberterrorism is defined by U.S. Federal Bureau of Investigation as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and subnational groups. The main aim behind cyberterrorism is to cause harm and destruction.

# Lecture 7

- Cyberterrorism can be explained as internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threaten individuals,certain groups, religions, ethnicities or beliefs.

**Cyberterrorism can be broadly categorized under three major categories:**

1. Simple: This consists of basic attacks including the hacking of an individual system.
2. Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
3. Complex: These are coordinated attacks that can have a large-scale impact and make use of sophisticated tools.

# Lecture 7

## Examples of cyberterrorism include:

- **Glo**bal terror networks disrupting major websites to create public nuisances/inconveniences or to stop traffic to websites that publish content the hackers disagree with.
- **Int**ernational cyberterrorists accessing and disabling or modifying the signals that control military technology.
- **Cyber**terrorists targeting critical infrastructure systems, for example, to disable a water treatment plant, cause a regional power outage, or disrupt a pipeline, oil refinery or fracking operation. This type of cyberattack could disrupt major cities, cause a public health crisis, endanger the public safety of millions of people as well as cause massive panic and fatalities.

# Lecture 7

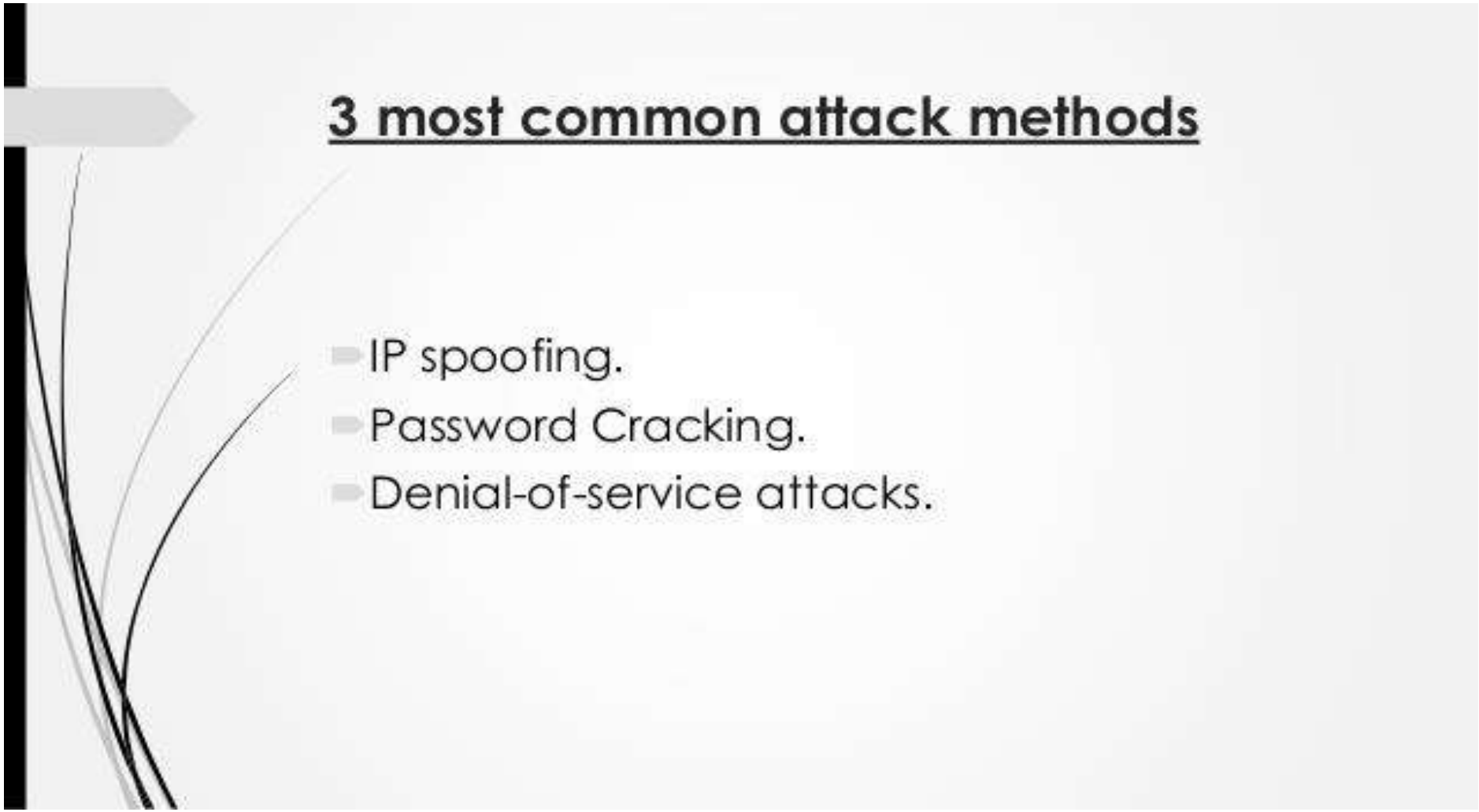
- Viruses, computer worms and malware targeting control systems can affect water supplies, transportation systems, power grids, critical infrastructure and military systems and may be used to further cyberterrorist goals.
- DoS attacks, cybersecurity events that occur when attackers take action to prevent legitimate users from accessing targeted computer systems, devices or other network resources.
- Hacking and theft of critical data from institutions, governments and businesses.

# Lecture 7

## How does Cyber Terrorism affect you and your future?

- **Air traffic** control towers or our airlines infrastructure could be hacked into.
- **Banking systems** could be violated and all of our money could be stolen.
- **Bombs** and other explosives could be set off by remote.
- **Hospitals** could lose all of their information.
- **Learn Government** secrets and plans
- **The tampering** of our water systems.

# Lecture 7


3 most common attack methods
IP spoofing.
Password Cracking.
Denial-of-service attacks.

# Lecture 7

## IP Spoofing

- Refers to creation of IP packets with forged source IP address with the purpose of concealing the identity of sender.
- Mostly used in Denial-of-Service attacks.
- Most effective in corporate networks where users can log in without a username or password.

# Lecture 7

## Password Cracking

- **Password cracking** can be implemented using brute-force attacks, Trojan horse programs and IP spoofing.
- Password attacks usually refer to repeated attempts to identify a user account and/or password; these repeated attempts are called brute-force attacks.
- One example is weak encryption(LM hash) used by Microsoft windows XP, can easily be attacked

# Lecture 7

## Denial-of-Service attacks

- **Denial-of-service attacks** focus on making a service unavailable to intended users.
- 2 forms of DoS attacks: those that crash services and those that flood services.
- One common attack method involves saturating the target machine with communications requests such that it cannot respond to the traffic.

# Lecture 7

## How does Cyber Terrorism affect you and your future?

- **Air traffic** control towers or our airlines infrastructure could be hacked into.
- **Banking systems** could be violated and all of our money could be stolen.
- **Bombs** and other explosives could be set off by remote.
- **Hospitals** could lose all of their information.
- **Learn Government** secrets and plans
- **The tampering** of our water systems.

# Lecture 8

## CYBER THREATS

What we will cover in this?

-Need for a comprehensive cyber security policy

# Lecture 8

# NEED FOR A COMPREHENSIVE CYBER SECURITY POLICY

# Lecture 8

## The need for a national cybersecurity policy framework

- The "Fourth Industrial Revolution" brings enormous economic and social opportunities for people, organizations, and governments.
- The substantial increase in internet connectivity, the explosion of the number of connected devices, and the rapid take-up of technologies such as cloud computing, advanced robotics, and artificial intelligence (AI) are fundamentally changing people's lives.

# Lecture 8

- At the same time, with every new system or device that is connected to the internet the scope for cyber-attacks grows, as do the consequences of successful attacks.
- As cyber-attackers become ever more sophisticated in their operations and cyber-criminals ever more ambitious, policymakers have to respond.

# Lecture 8

- The Cybersecurity Policy Framework is designed for policy-makers involved in the development of cybersecurity regulations.
- It is not intended to exhaustively address all of the key parts of a country's national or international cybersecurity strategy but, rather, to provide a practical guide to the specific areas of cybersecurity regulation that policy-makers are currently most focused on.

# Lecture 8

- Cybersecurity Policy Framework focuses on three key regulatory aspects of cybersecurity policy, framed by a wider national strategy as well as an international strategy for cybersecurity.

# Lecture 8

# INTRODUCING KEY CONCEPTS IN CYBERSECURITY POLICY

# Lecture 8

The protection of connected systems and networks, and the data stored on those systems and transferred via those networks, from attack, damage or unauthorized access.

# Lecture 8

## CYBERSECURITY NORMS

- Agreed expectations for the behavior of state actors in cyberspace at an international level - e.g., the need for states to cooperate in preventing international cybercrime.

# Lecture 8

## Critical Infrastructure (CI)

Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

**Information security**

Protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

**Security Baselines**

The minimum security standards required for information security systems.

# The steps involved in ensuring information security

**International standards**

Typically refers to international security standards, such as ISO/ IEC standards, against which organizations can measure their security practices.

# Critical information infrastructure (CII)

Information and communication systems forming part of CI (see above) whose maintenance, reliability and safety are essential for the proper functioning of the CI and/or the country as a whole.

**Security controls**

Specified measures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

**What is a national strategy for cybersecurity?**

A national cybersecurity strategy outlines a country's cybersecurity vision and sets out the priorities, principles, and approaches to understanding and managing cybersecurity risks at a national level

## Why is a national strategy for cybersecurity needed?

Any regulatory framework for cybersecurity needs be based upon a principled national strategy. The national strategy should set clear, top-down direction to establish and improve cybersecurity for government, organizations, and citizens.

Such a strategy is essential for managing national-level cybersecurity risks and for developing appropriate regulation to support those efforts.

# What is a national cybersecurity agency?

Many countries around the world have established, or are looking to establish, civilian agencies or other administrative bodies to manage the country's cybersecurity strategy.

Countries as diverse as Australia, France, Israel, Japan and Singapore, to name just a few, already have specific bodies of government responsible for cybersecurity.

The move towards establishing national cybersecurity agencies reflects the increased inter-dependencies caused by the digital transformation, as well as the perceived and real growth of cyber-threats.

**Why is a national cybersecurity agency needed?**

Because cybersecurity touches all aspects of our society, establishing a well-functioning agency will benefit the broader cybersecurity ecosystem.

These type of agencies have unique authorities that allow them to address cybersecurity directly, but also perform an essential function in coordinating across different organizations in the country - government and private.

As governments around the world begin to consider creating or restructuring their own national cybersecurity agencies, this Cybersecurity Policy Framework offers a set of best practices to guide their development.

**The four recommendations for structuring an effective national cybersecurity agency are:**

Appoint a single national cybersecurity agency

Provide the national cybersecurity agency with a clear mandate

Ensure the national cybersecurity agency has appropriate statutory powers

Implement a five-part organizational structure

- Policy and planning unit
- Outreach and partnership unit
- Communications unit
- Operations unit
- Regulatory unit

## Objective

Ministry of Communications and Information Technology (India) define objectives as follows:

To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.

To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).

To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

**Strategies**

Creating a secured Ecosystem.

Creating an assurance framework.

Encouraging Open Standards.

Strengthening The regulatory Framework.

Creating mechanism for Security Threats Early Warning, Vulnerability management and response to security threat.

Securing E-Governance services.

Protection and resilience of Critical Information Infrastructure.

Promotion of Research and Development in cyber security.

Reducing supply chain risks

Human Resource Development (fostering education and training programs both in formal and informal sectors to support Nation's cyber security needs and build capacity.

Creating cyber security awareness.

Developing effective Public Private Partnership.

To develop bilateral and multilateral relationship in the area of cyber security with other country. (**Information sharing and cooperation**)

Prioritized approach for implementation

Need for a Nodal Authority

National Cyber Security Policy (2013) provides for developing effective Public Private Partnership and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

A Joint Working Group (JWG) for Public Private Partnership on cyber security has been set up at NSCS which is working in following areas:

Setting up of **Information Sharing and Analysis Centres** (ISACs) in critical sectors like Banking, Telecommunications and Power.

Establishment of **Centres of Excellence** (CoEs) on Policy Research, Standards, Audit.

Capacity building for law enforcement agencies and cyber forensics.

Establishment testing labs for telecom and IT equipment under **Public-private partnership** (PPP) model

The following mechanism and measures are in place to ensure digital safety and cyber security:

Indian Computer Emergency Response Team (CERT-In) is designated as a National nodal agency to coordinate matters related to cyber security incidents in the country.

National Critical Information Infrastructure Protection Centre (NCIIPC) has been setup to enhance the protection and resilience of Nation’s Critical information infrastructure.

Government has issued general guidelines for **Chief Information Security Officers** (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance Organisations are encouraged to develop their organisation level cyber security policy.

Public Private Partnership has been developed for cooperation and collaboration for responding cyber security incidents.

Awareness has been created in law enforcement agencies through conducting cybercrime awareness workshops.

Information Security Education and Awareness (ISEA) Project is being implemented with an objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness.

The project aims to train 1.14 Lakhs persons under Academic activities (formal and non-formal courses) by the year 2020.

So far more than 71000 candidates have been trained in various formal/non-formal courses in Information Security through 52 academic and training institutions.

Cyber forensics training labs in all north eastern states, CBI Academy Ghaziabad and cities such as Mumbai, Pune,Kolkata and Bangalore have been setup and more than 28,000 state police from North Eastern States, Maharashtra, West Bengal and Karnataka have been trained for dealing with cybercrime.

Cyber Crisis Management Plan (CCMP) for countering cyber threats and cyber terrorism has been developed and so far 60 workshops have been conducted for Central Govt. Ministries/Departments, States/Union Territories and other organisations.

Research and development is carried out in the thrust areas of cyber security including (a) Cryptography and cryptanalysis, (b) Network & System Security, (c) Monitoring & Forensics, and (d) Vulnerability Remediation & Assurance through sponsored projects at recognized R&D organizations.

Government has initiated setting up of **National Cyber Coordination Centre (NCCC)** to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) which provides detection of malicious programs and free tools to remove the same.

## Introduction

CERT-In is a functional organisation of Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

## Vision

Proactive Contribution in Securing India's cyber space.

## Mission

To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.

## Objectives

- Preventing cyber attacks against the country's cyber space.
- Responding to cyber attacks and minimizing damage and recovery time Reducing 'national vulnerability to cyber attacks.
- Enhancing security awareness among common citizens.

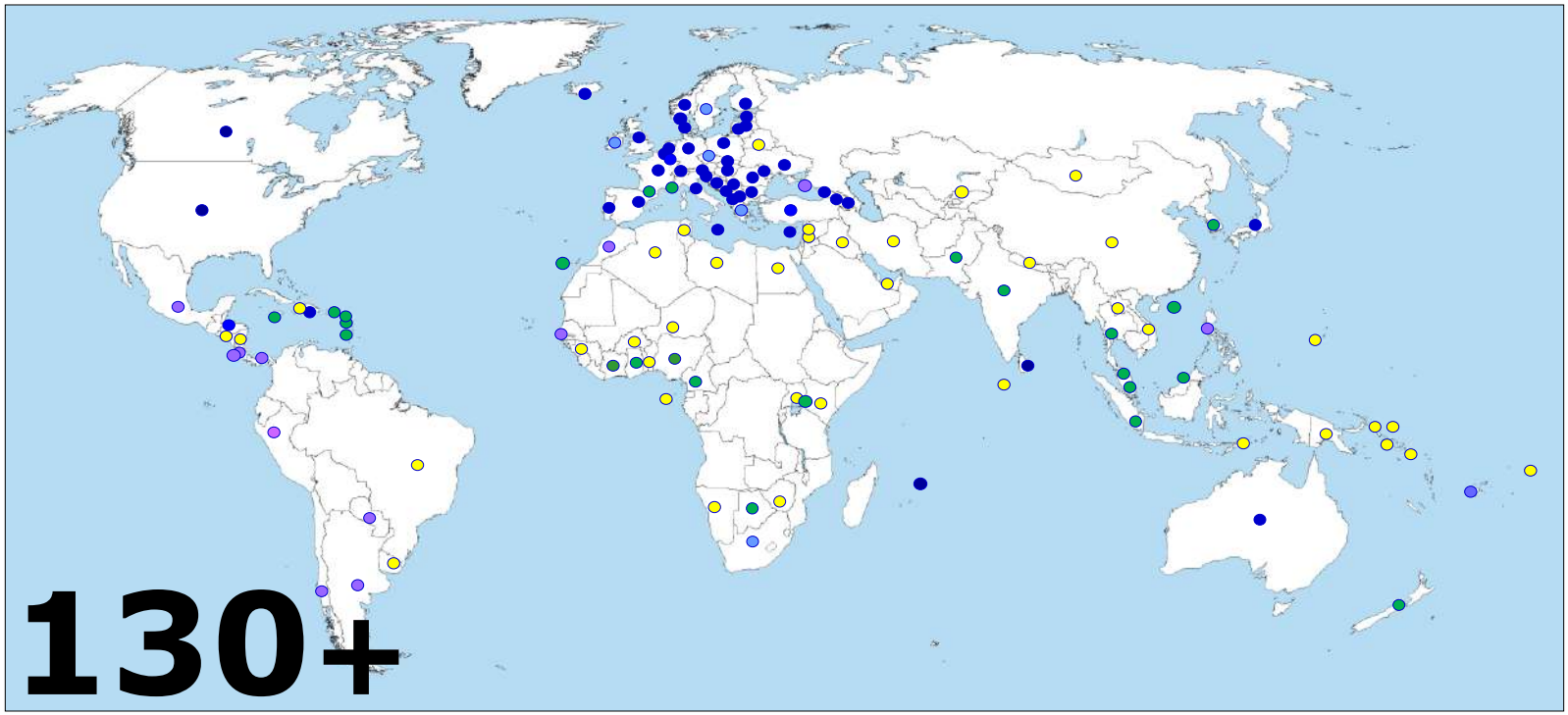
## Functions/Activities (allocation of Business Rules)

The Information Technology (Amendment) Act 2008, designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

# Need for an International convention on Cyberspace

# Reach of the Budapest Convention / reach of capacity building




Indicative map only

**Budapest Convention**

**Ratified/acceded: 50**

**Signed: 5**

**Invited to accede: 11**

**= 66**

49

6

11

**Other States with laws/draft laws largely in line with Budapest Convention = 20**

**Further States drawing on Budapest Convention for legislation = 45+**

# About the Budapest Convention on Cybercrime

**Opened for signature in Budapest, Hungary, in 2001**

**By 1 December 2016:**

- **50 Parties (European, Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, USA)**
- **5 Signatories (European, South Africa)**
- **11 States invited to accede (Argentina, Chile, Colombia, Costa Rica, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal, Tonga)**

**= 66 States**

# Budapest Convention: scope

**Criminalising conduct**

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

**Procedural tools**

- Expedited preservation
- Search and seizure
- Interception of computer data

+

**International cooperation**

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

**The only binding international instrument and guiding legislative tool in the fight against Cybercrime**

# Budapest Convention: The role of the Cybercrime Convention Committee (T-CY)

(Committee of Parties to the Budapest Convention)

**Established under Article 46 Budapest Convention**

## Membership (November 2016):

- 50 Members (State Parties)
- 17 Observer States
- 12 organisations (African Union Commission, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

## Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments

Two plenaries/year as well as Bureau and working group meetings

- An effective follow-up mechanism;
- The T-CY appears to be the main inter-governmental body on cybercrime matters internationally

# GLACY

Global Action on Cybercrime
Action globale sur la cybercriminalité

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

**To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.**

## OBJ 1: CYBERCRIME AND CYBERSECURITY POLICIES AND STRATEGIES

- To promote consistent cybercrime and cyber security policies and strategies.

## OBJ 2: POLICE AUTHORITIES AND INVESTIGATIONS

- To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.

## OBJ 3: CRIMINAL JUSTICE AND INTERNATIONAL COOPERATION

- To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

# GLACY+ : Project Management and Implementation matters 1/2

- **INTERPOL** will be implementing partner for all activities related to law enforcement capacities (Objective 2)
- All activities will be carried out through the establishment and proactive support of **GLACY+ national Coordination Teams**
    - Importance of a structured National Coordination Team (Law Enforcement, Judicial Service, Prosecuting Authority, ICT National Agency, MFAs, CERTS)
- Involvement of **Project Partners** in activities relevant to expertise and competencies
    - Romania, France, Europol EC3, UK NCA, USA, Estonia

# GLACY+ : Project Management and Implementation matters 2/2
# GLACY+: Gestion du Projet et matières de mise en œuvre

- Full alignment with the **European Commission** on goals, workplan and intermediate achievements of the project
- Involvement of the **EUDs** in each mission
- Stronger involvement of regional organizations or other international institutions:
- ECOWAS, GFCE, AUC, ASEAN, OAS, UNODC, UNAFRI, GPEN...
- Two co-managers in conjunction of efforts and a support team composed by 2 Project Officers and 2 Project assistants, with possibility for enlargement

# Capacity building on cybercrime: lessons learnt

## Factors of success:

- Capacity building backed up by common standards (example: Budapest Convention) and follow up mechanism (example: Cybercrime Convention Committee of the Parties- T-CY)
- Political commitment to implement standards (Example: signature or formal request for accession to Budapest Convention) as a prerequisite for full range of support)
- Rule of law conditions: strengthening legislation, including safeguards for procedural powers, as starting point
- Sequencing of activities: Initial situation reports ▶ committing decision makers and counterpart organisations ▶ implementing activities ▶ assessing progress made ▶ feeding results back into policies
- Country project teams ▶ Example GLACY/GLACY+: cooperation with 7 x 5 institutions
- Capacities for capacity building ▶ C-PROC

# Capacity building on cybercrime: lessons learnt

## Obstacles:

- Difficulties in obtaining electronic evidence; The issue of Artº 32 of the Budapest Convention;
- International cooperation difficulties and inabilities; Lack of capacity in States to Cooperate;
- Gaps in Legislation;
- Lack of training;
- Lack of technological means;
- And many, many others…. A long run to a stabilization and synergy of efforts in the fight against cybercrime.

# Upcoming Capacity building programme for MENA region - CYBERSOUTH

## CYBERSOUTH:

### OBJECTIVES:

- Criminal Law frameworks strengthened in line with the Budapest Convention on Cybercrime including Rules of Law Safeguards;;
- Specialized police and prosecution services and interagency cooperation strengthened;
- Judicial training on cybercrime and electronic evidence mainstreamed;
- More efficient international cooperation;
- Cybercrime and cybersecurity policies and strategies strengthened;

### GEO SCOPE:

MENA Region (Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia) – May 2017-April 2020


Thank You