CYBERSPACE & CYBERCRIME MONITORING FRAMEWORK, POLICY & PROTOCOLS

Cyberspace, amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure. As opposed to the Internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state.

It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants. Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.**
- **Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.**
- **Information security protects the integrity and privacy of data, both in storage and in transit.**
- **Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and**

the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- **Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.**
- **End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.**

DEVELOPING A LEGAL FRAMEWORK TO COMBAT CYBERCRIME

Providing Law Enforcement with the Legal Tools to Prevent, Investigate, and Prosecute Cybercrime

- **Balancing Privacy and Public Safety**
- **Limits on Law Enforcement Investigative Authority**
- **Intercepting Electronic Communications**
- **Collecting Traffic Data Real Time**
- **Obtaining Content Stored on a Computer Network**
- **Obtaining Non-Content Information Stored on a Computer Network**
- **Compelling the Target to Disclose Electronic Evidence**

CYBERCRIME POLICY

Top 10 Most Effective Cybercrime Policies

- **Engage in internal employee monitoring.**
- **Have a written inappropriate-use policy.**
- **Require employees and contractors to sign acceptable-use policies.**
- **Monitor Internet connections.**
- **Require internal reporting to management of insider misuse and abuse.**
- **Host employee education and awareness programs.**
- **Develop a corporate security policy.**

- **Conduct new employee security training.**
- **Do periodic risk assessments.**
- **Conduct regular security audits.**

Areas that are related to cyber law include cyber-crime and cyber security. With the right cyber security, businesses and people can protect themselves from cyber-crime. Cyber security looks to address weaknesses in computers and networks. The International Cyber Security Standard is known as ISO 27001.

Cybersecurity policy is focused on providing guidance to anyone that might be vulnerable to cybercrime. This includes businesses, individuals, and even the government. Many countries are looking for ways to promote cybersecurity and prevent cybercrime. For instance, the Indian government passed the Information Technology Act in 2000. The main goal of this law is to improve transmission of data over the internet while keeping it safe.

Information is another important way to improve cybersecurity. Businesses, for example, can improve cybersecurity by implementing the following practices:

- **Offering training programs to employees.**
- **Hiring employees who are certified in cybersecurity.**
- **Being aware of new security threats.**

Cybercrimes can be committed against governments, property, and people.

"Cyber ethics" refers to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life with lessons such as "Don't take what doesn't belong to you" and "Do not harm others," we must act responsibly in the cyber world as well.

Ethics — moral principles that govern a person's behavior — is a critical part of any sound cybersecurity defense strategy. Without clear ethical standards and rules, cybersecurity professionals are almost indistinguishable from the black-hat criminals against whom they seek to protect systems and data.

RESPONSIBLE AI

Responsible AI is a framework for bringing many of these critical. practices together. It focuses on ensuring the ethical, transparent and accountable use of AI technologies in a manner consistent with user expectations, organizational values and societal laws and norms.

There are 3 types of artificial intelligence (AI): narrow or weak AI, general or strong AI, and artificial superintelligence.

IS AI UNETHICAL?

If artificial or alien intelligences show evidence of being sentient, this philosophy holds that they should be shown compassion and granted rights. Joanna Bryson has argued that creating AI that requires rights is both avoidable, and would in itself be unethical, both as a burden to the AI agents and to human society.