Professional Certificate in International Cyber Law

Internet Governance and Policy

Cyberlaw: The body of law governing the use of the Internet and other computer networks. It covers a wide range of issues, including intellectual property, privacy, freedom of expression, and cybercrime.

Internet Governance: The development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet. It involves a range of stakeholders, including governments, private sector entities, civil society organizations, and technical communities.

Internet Service Provider (ISP): A company that provides access to the Internet. ISPs can be classified into different types, such as wired, wireless, and satellite, based on the technology they use to provide access.

Domain Name System (DNS): A system that translates domain names into IP addresses, allowing users to access websites using human-readable names instead of numerical addresses. The DNS is a critical infrastructure of the Internet and is governed by a complex set of policies and procedures.

Cybersecurity: The practice of protecting Internet-connected systems, including hardware, software, and data, from theft, damage, or unauthorized access. Cybersecurity involves a range of measures, such as firewalls, antivirus software, and user education, to prevent and mitigate cyber threats.

Cybercrime: Criminal activities that use the Internet or other computer networks as a medium or a target. Cybercrime includes a wide range of offenses, such as hacking, phishing, identity theft, and online fraud.

Intellectual Property: Creations of the mind, such as inventions, literary and artistic works, and symbols, names, and images used in commerce. Intellectual property rights, such as patents, copyrights, and trademarks, give creators exclusive rights to use, sell, or license their creations for a certain period.

Privacy: The right to control the collection, use, and dissemination of personal information. Privacy is a fundamental human right recognized in many legal instruments, including the Universal Declaration of Human Rights and the European Convention on Human Rights.

Freedom of Expression: The right to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, or in print, in the form of art, or through any other media of his choice. Freedom of expression is a fundamental human right recognized in many legal instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Net Neutrality: The principle that Internet service providers should treat all Internet traffic equally, without discriminating or charging differently based on the source, destination, or content of the traffic. Net neutrality is a critical principle for maintaining the openness and freedom of the Internet.

Artificial Intelligence (AI): The ability of a machine to perform tasks that would normally require human

intelligence, such as visual perception, speech recognition, decision-making, and language translation. AI has many potential applications in cyberlaw and policy, such as identifying and preventing cyber threats, automating legal processes, and promoting access to justice.

Blockchain: A decentralized, distributed database that records transactions on multiple computers. Blockchain technology is the underlying technology of cryptocurrencies, such as Bitcoin, but has many other potential applications, such as supply chain management, digital identity, and smart contracts.

Cyber Diplomacy: The use of diplomatic means to address issues related to cybersecurity, cybercrime, and Internet governance. Cyber diplomacy involves a range of activities, such as negotiations, dialogues, and confidence-building measures, to promote cooperation and trust among states and other stakeholders.

Data Protection: The measures taken to protect personal data from unauthorized access, use, or disclosure. Data protection is a critical aspect of privacy and is governed by a complex set of legal and technical measures.

Digital Divide: The gap between individuals, households, businesses, and regions that have access to digital and Information and Communication Technologies (ICTs) and those that do not. The digital divide is a significant challenge in many parts of the world, particularly in developing countries, and is a key focus area for Internet governance and policy.

E-commerce: The buying and selling of goods and services over the Internet. E-commerce has grown rapidly in recent years, driven by the widespread adoption of the Internet and mobile devices.

Encryption: The process of converting plain text into a coded format that is only accessible to authorized parties. Encryption is a critical tool for protecting the confidentiality, integrity, and authenticity of digital communications and transactions.

Hacking: The unauthorized access, use, disclosure, disruption, modification, or destruction of computer systems, networks, or electronic data. Hacking is a criminal offense and a significant challenge for cyberlaw and policy.

Internet of Things (IoT): A network of interconnected devices, objects, and systems that are embedded with sensors, software, and other technologies to collect and exchange data. The IoT has many potential applications, such as smart homes, smart cities, and industrial automation, but also poses significant challenges for cybersecurity and privacy.

Jurisdiction: The legal authority of a state or other entity to exercise power or authority over a person, organization, or activity. Jurisdiction is a key issue in cyberlaw and policy, as the borderless nature of the Internet raises questions about the territorial limits of legal authority.

Malware: Software that is designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Malware includes a wide range of threats, such as viruses, worms, Trojan horses, and ransomware.

Phishing: The practice of sending fraudulent emails or messages that appear to be from reputable sources,

with the aim of tricking recipients into revealing sensitive information, such as passwords or credit card numbers. Phishing is a common form of cybercrime and a significant challenge for cyberlaw and policy.

Privacy by Design: An approach to the design and development of technology that prioritizes privacy and data protection. Privacy by Design involves integrating privacy considerations into all stages of the technology development process, from conception to deployment.

Spam: Unsolicited, often commercial, messages that are sent in bulk over the Internet. Spam can be a nuisance and a security risk, as it can be used to spread malware or phishing scams.

State Sovereignty: The principle that states have exclusive authority over their territory, people, and resources. State sovereignty is a key principle of international law and is often invoked in debates about Internet governance and cybersecurity.

Two-Factor Authentication: A security measure that requires users to provide two forms of identification before accessing an account or system. Two-factor authentication typically involves something the user knows, such as a password, and something the user has, such as a physical token or a mobile device.

Virtual Private Network (VPN): A secure, encrypted connection between two or more devices over the Internet. VPNs are commonly used to protect privacy and security, as they allow users to browse the Internet anonymously and access geographically restricted content.

Website Terms of Service: The rules and regulations that govern the use of a website or online service. Website terms of service typically cover issues such as user conduct, intellectual property, and liability.

Zero-Day Exploit: A software vulnerability that is unknown to the software vendor or security community. Zero-day exploits are often used by hackers to gain unauthorized access to computer systems or networks, as there is no patch or fix available to prevent the attack.

Cyber Terrorism: The use of the Internet or other computer networks to carry out acts of terrorism, including the threat or use of violence, with the aim of causing fear, harm, or disruption. Cyber terrorism is a significant challenge for cyberlaw and policy, as it poses a threat to national security, critical infrastructure, and individual safety.