What is Cybersecurity?

The term ‘Cyber Security’ commonly refers to the safeguards and actions that can be used to protect the cyber domain and preserve the integrity of the Internet infrastructure and the confidentiality of information contained therein.

Cybersecurity Policy Making Challenges

- Failure of policy makers to adequately understand and adapt to the nature of cyber domain (rapidity of change, lack of familiarity with the technology under development, unpredictability of future developments).
- The features of cyberspace challenge the conventional models of regulation based on the principles of sovereignty and territoriality => The centre of gravity has shifted from public to private sector, which owns and operates significant parts of cyberspace.
- Protection of cyberspace-reliant societies against cyberthreats vs. Openness of the Internet as a platform for innovation and new sources of growth & Respect of fundamental values (privacy, freedom of speech, free flow of information).
- Need for co-operation between governments, private sector and the Internet technical community at a national and international level.
- Need for a holistic approach to cybersecurity policy making encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects.

An Economic Approach to Cybersecurity

- The role of Business Models and Incentives is critical in the decision making process
- Internet Intermediaries operate under an incentive structure which consists of contradictory forces, others enhancing security (positive incentives), others working against it (negative incentives)
- Positive Incentives (e.g. loss of reputation and brand damage, building customer loyalty, potential costs of customer support and abuse management)
- Negative Incentives (e.g. costs of increasing security, price competition)
- Alternative mechanisms needed (e.g. price-sharing scheme in which all market players will share the costs, public-private partnerships, government subsidies, development of industry-led standards for companies’ performance)

Internet Intermediaries

Internet technology requires the insertion of intermediaries, such as Internet access and service providers, web hosting providers, search engines, e-commerce intermediaries, payment systems, and participative networked platforms - parties which bring together or facilitate interactions and transactions between third parties on the Internet, provide access to, host and transmit content generated by third parties, or provide Internet-based services to third parties.

Legal Liability in cyberspace differs from that in the offline world. Fault-based notions of responsibility cannot apply to cyberspace => Third-party liability as an alternative solution

Internet Intermediaries have the technical expertise required to implement the appropriate security techniques to thwart attacks that violate Internet’s integrity and security

Security Techniques & Limitations

- BCP38: a packet filtering technique intended to limit the impact of DDoS attacks by denying access to the network to traffic with spoofed addresses and by helping to ensure that traffic is traceable to its correct source network. BUT Easily circumvented, Risk of under- or over-blocking.
- Deep Packet Inspection: a type of data processing that looks in detail at the contents of the data being sent and re-routes it accordingly, making sure that a feed of data is supplying content in the right format, or is free of viruses. BUT Privacy, Transparency & Confidentiality issues.
- Quarantining: infected machines are placed in quarantine, prevented from accessing the Internet, until they receive a ‘health certificate’. BUT High risk of cutting off innocent users, Need to keep the Internet open.