Cybersecurity

AL Mansour University College

Digital Media Department

4th Class

Lecturer Mustafa Muhanad

-3-

1. 7. Cybersecurity Challenges

All stakeholders agree on the importance of cybersecurity. As it known, only secure and reliable cyberspace can generate and preserve trust in the Internet. With the development of the Internet and new technologies, cybersecurity has become more complex.

The following issues some of the main challenges of cybersecurity:

1- Privacy: Cybersecurity and privacy are often intertwined and interdependent. They impact trust in the digital space and may limit its potential for growth and prosperity.

2- The Internet architecture: The very nature of its organization affects the security of the Internet. Most past developments in Internet standards have been aimed at improving performance or introducing new applications; security was not a priority. The Internet Engineering Task Force develops and promotes Internet standards.

3- Electronic commerce: Cybersecurity is often mentioned as one of the prerequisites for the rapid growth of e-commerce. Without a secure Internet, customers will be reluctant to provide confidential information online, such as credit card numbers.

4- Internet of Things: The Internet of Things is the key driver of the digital revolution and creates new opportunities for our society, such as new products and services, but also creates vulnerabilities. Cybersecurity is a basic requirement for trust in the Internet of Things, as vulnerabilities could undermine the trust of individual users and society as a whole.

5- Legal & Regulatory issues: Cybersecurity norms could be viewed as an important mechanism for state and non-state actors to agree on a responsible way to behave in cyberspace.

6- Cybersecurity Best Practices: The successful implementation of a collaborative model for cybersecurity strategy development and implementation resides in agile adaptability, transparency, and trusted information sharing among and between all participants. Participation should extend not only to public and private sector entities but also to stakeholders from other sectors (e.g., the banking and finance sectors, business process outsourcing (BPO), health, tourism, and energy sectors) and non-profit stakeholder groups (e.g., the technical community, academia, and civil society).

1. 8. Cyber Threats

A cyberattack is best understood not as an end in itself but as a means to a wide variety of other ends, some of which have tangible political, military, criminal, and social consequences.

A cyberattack is not a strategy but a tactic that may be employed as one of many other cyber and non-cyber tactics toward the attainment of a broader strategy. A cyber attacker's ultimate goal could be anything from personal amusement to intellectual property theft to political revolution, terrorism, or even international war.

In this section, five types of cyber espionage, crime, activism, terrorism, and war are explored.

1. Cyber Espionage: In this type, a hacker does not do anything to data, except take it and read it. However, the amount of data that hackers can steal has already made this generation the Golden Era of Espionage. And as more and more of our lives are played out online, and as once-isolated computers are connected to the Internet, the level of sensitivity of the stolen data continues to rise.

2. Cyber Crime Criminals: those criminals are no strangers to technology. Counterfeiting. Today, counterfeiters likely have it much easier, as both money and intellectual property exist in electronic bits that can be transmitted around the world at light speed.

3. Cyber Activism: is the process of using Internet-based socializing and communication techniques to create, operate and manage activism of any type. It allows any individual or organization to utilize social networks and other online technologies to reach and gather followers, broadcast messages and progress a cause or movement.

4. Cyber Terrorism: Cyber-terrorism involves the use of computers and/or related technology to cause harm or damage, to coerce a civilian population, and influence the policy of the target government or otherwise affect its conduct. Furthermore, cyber-terrorism which should be differentiated from hacktivism and cyber-warfare implies targeting Critical Infrastructures. There are linkages as well as discrepancies between cyber-terrorism and terrorism broadly speaking, which unavoidably affect the counterterrorism response in either case.

5. Cyberwarfare: involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.