Cyber Security: A Brief Encounter

Anil Kumar Pandey*

I. Introduction

The digital domain has become more intertwined with our daily lives. Citizens, government bodies and businesses are using digital applications for online interactions, transactions, more efficient collaboration communication and entertainment. More equipment with integrated ICT services is connected to the internet: computers and telephones, but also cars, thermostats and medical equipment. This increasing digitization is not only for ease, efficiency and pleasure, but is also an important drive behind innovation and economic growth.

Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems. There is a wide range of currently accepted cyber security definitions:

1. The Committee on National Security Systems defines cyber security as the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or, destroying the integrity of the data or stealing controlled information.
2. The National Institute of Standards and Technology defines cyber security as "the process of protecting information by preventing, detecting, and responding to attacks." Similar to financial and reputational risk, cyber security risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.
3. International Organization for Standardization defines cyber security or cyberspace security as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form." At its core, cybersecurity seeks to protect your enterprise from those who wish to do harm to your business, steal your information or your money, or use your systems to target peers in the market.

Cybersecurity is a shared responsibility – people, processes, tools, and technologies work together to protect an organization's assets. Protecting your organization's assets requires a focus on the following three fundamental goals:

A. Confidentiality Any important information you have that should be kept confidential. This information should only be accessed by people (or systems) that you have given permission to do so.
B. Integrity Maintain the integrity of information assets to keep everything complete, intact, and uncorrupted.
C. Availability Maintain the availability of systems, services, and information when required by the business or its clients.

II. Strategic Objectives

1. FUNDAMENTAL INTERESTS,DEFENSE AND SECURITY OF STATE INFORMATION SYSTEMS AND CRITICAL INFRA-STRUCTURES, MAJOR CYBER SECURITY CRISIS.(Having the scientific, technical and industrial capabilities required to protect sovereign information, ensure cyber security and develop a trustworthy digital economy.)
2. DIGITAL TRUST, PRIVACY,PERSONAL DATA, CYBERMALEVOLENCE(Measuring cybercrime, Recommending technical solutions aimed at securing digital life and which are accessible to all businesses and the general public. Reinforcing the operational mechanisms of legal international mutual aid and universalizing the principles of the IT ACT 2000/1TA 2008)

Anil Kumar Pandey*
B.E. (Electronics) LL.b., PgD. Cyberlaws and IPR (Central University, Hyderabad)

3. RAISING AWARENESS, INITIALTRAINING, CONTINUING EDUCATION (Integrating cyber security awareness into all higher and continuing education programmes. children's awareness of digital security and responsible cyberspace behaviors' as 'of school age. Initial higher education and continuing education will include a section dedicated to digital security adapted to the sector.)
4. THE ENVIRONMENT OF DIGITAL TECHNOLOGY BUSINESSES, INDUSTRIAL POLICY, EXPORT AND INTERNATIONALISATION (Develop an environment that is favorable to research and innovation and will make digital security a factor in competitiveness. It will support the development of the economy and the international promotion of its digital products and services. It will ensure that digital products and services with levels of ergonomics, trust and security adapted to the uses and cyber threats are available to its citizens, businesses and administrations.)
5. DIGITAL STRATEGIC AUTONOMY, CYBERSPACE STABILITY

III. Cyber Insurance

Information sharing and advanced cyber security technologies will not stop all cyber attacks—by now it seems clear that technically adept adversaries will always find new ways to circumvent cyber security safeguards. That's why many businesses are purchasing cyber security insurance to help Mitigate the financial impact of cybercrimes when they do occur. Cyber security insurance is, in fact, one of the fastest-growing sectors in the insurance market: cyber insurance market will reach$7.5 billion in annual sales by 2020,up from $2.5 billion this year. Today, first-party insurance products cover data destruction, denial of service attacks, theft and extortion; they also may include incident response and remediation, investigation and cyber security audit expenses. Other key areas of coverage include privacy notifications, crisis management, forensic investigations, data restoration and business interruption. The insurance industry is attempting to expand into policies that cover the value of ostntellectual property, reputation and brand image, as well as cyber related infrastructure failures.

IV. Challenges

Future developments in cyber security are hard to predict. However, a clear picture can be painted of the Challenges which currently and in the long-term influence the security and openness of the digital domain:

- The Internet of Things (everything is connected to the internet) and hyper connectivity (everything is connected to each other) promotes innovation and results in usability. At the same time, it raises the question of whether or not digitally linked products and services are actually safe and what the implications may be for privacy.– The amount of data available in digital form is only increasing; as will the interest in acquiring such data. Governments and businesses, increasingly working with large data files, which are also increasingly stored in the cloud, are faced with increased risks.
- The playing field in the digital domain is not only determined by states, but also by major private market parties. Governance in the digital domain is therefore complex and cannot always be solved in traditional forums, as it requires a multi-stakeholder approach. This applies to security standards as well as to the protection of fundamental rights and values.
- In the cyber domain, we see an increasingly interwovenness of civil and military domains due to substantial mutual dependence on similar ICT systems and application and the complex attribution issue. we have to take into consideration that civil targets prone to cyber attacks. Furthermore, in case of large-scale attacks, the Defense organization's cyber capabilities may be called upon to protect the vital national civil infrastructure. In view of the above, clear Parameters for strengthened cooperation in the digital domain are needed.
- The increased complexity and dependence on ICT-based products and services require a higher level of expertise. This both concerns the level of expertise of average internet users and sufficiently-qualified experts.