BPF –Cyber Security

How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Cybersecurity refers to the measures taken to protect computerized systems against unauthorized access or attack. Good cyber is good business. Almost 4 billion people are connected to the internet through cyberspace. Implementing Cybersecurity protects the system against viruses, worms, spyware and other unwanted programs. It protects the computer from being hacked and it gives privacy to the users.

Due to the huge development of the cyber space, the political, economic and societal forces both booster as well as hinders technological progress and growth of cybersecurity. From a security and privacy perspective, introduction of sensors and devices into currently intimate spaces – such as the home, the car,and with wearables and ingestibles, even the body is challenging. Therefore good cybersecurity contributes to the growth of and trust in ICTs in the field of telemedicine, disease monitoring and the storage of patient data also.

How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Cyber-attacks is causing increasing damage to companies, government and individuals. In 2010, Stuxnet worm targeted industrial control systems.In 2012, Shamoon virus targeted energy sector infrastructure. In May 2017, Ransom ware inscribed itself around 300,000 computers. Criminals are really good at focusing IT Systems. New hacking threats have emerged in past two to three years. The attacks are progressively destructive. Internet is utilized for terrorist purposes. Terrorists'organizations may develop virtual messages, presentations, magazines, audio and video files and video games. There are some risks that involve direct collection of sensitive personal information such as precise geolocation, financial account numbers, or health information. Other potential problems faced include issues such as denial of service attacks that can affect progress towards this goal. Firewalls can be difficult to configure correctly.Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly. It makes the system slower than before. Discussed above are few outcomes of poor cybersecurity.

Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges?

Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services

Denial of Service attacks is not used to gain unauthorized access or control of a system. They are designed to render it unusable. Attackers can deny service to individual victims by entering a wrong password for consecutive times to cause the victim account to be locked or block all users at once. Distributed denial of service (DDoS) attacks are very common, where a large number of hosts are used to flood a target system with network requests, thus attempting to render it.unusable through resource exhaustion.

Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments

The mobile technology is increasing very rapidly. The information can be shared anywhere and at any time. The quick adoption of smartphones reflects movement towards an internet based security including the internet of things. The mobile internet subscriptions increase by 60 percent in developed countries and by a 400 percent in developing countries. The loss of a single smart device not only means the loss of information, but increasingly it also leads to a loss of identity The strong economic conditions will create favorable environments for investment in research and development, which can further increase the economic growth by creating business opportunities and increasing productivity.

Considering the payment part smart payments have become a part and parcel of life. Maybe a Mall or supermarket or Toll gate nowadays payments happen within a fraction of second through smart devices. Without smart devices life seems to be crippled.

Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended

Information and Communications Technologies (ICTs) have greatly enhanced our capacities to collect, store, process and communicate information. It make us vulnerable to intrusions of our privacy. Data on our own personal computers can compromise us in unpleasant ways. Transmission of data over the Internet and mobile networks is equally fraught with the risk of interception- both lawful and unlawful that could compromise our privacy. In this age of cloud computing, our emails, chat logs, personal profiles, bank statements, etc., reside on distant servers of the companies whose services we use, and our privacy becomes stronger.There are a number of technological measures through which these risks can be reduced.

Confidentiality and availability of sensitive information, in particular in medical and health services

Physical devices like cars, medical devices are also connected to Internet including laptops and mobile phones. In future, over 50 billion objects are expected to be connected to the internet. For example, without going to the doctor’s office. Insulin pumps and blood-pressure cuffs can be connected to a mobile app which enable the people to record, track, and monitor their own vital signs. This especially benefits the aging people who can manage the health care at home without the need for long-term hospital stays. Sophistication and engineering designs of advanced devices and software can help sharing of medical and health information with privacy and confidentiality.

Online abuse and gender-based violence

Encouraging gender diversity in the cybersecurity field will contribute to developing a qualified cybersecurity workforce as well as to deliver cybersecurity solutions.Gender-based violence refers to cyber violence, online violence and technology-related violence against women.Online abuse and gender-based violence affect particularly the girls of age group of 18 years and below. This issue may occur due to the lack of awareness among young people.

Harassment includes the use of abusive comments, verbal online abuse, etc. Eg: Sagarika Ghose and her husband, Rajdeep Sardesai, are both well-known journalists and active Twitter users in India. While both receive frequent criticism and abuse on Twitter for their views, the format such abuse takes is notably gendered .Effective measures has to be taken to construct a safe and secure environment for women and girls in all aspects of life. Creating awareness about the safe use of internet, social media and online violence against women and girls. Disable the links that is violence against women and girls.

Security risksof shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities

The companies should develop the security policies and procedures and identify the risks related to cyber security. They should be able to detect unauthorized activity. The DNS system is exposed to threats that aim to bring down a central feature which allows convenient web browsing for non-technical users and enables flexible addressing for automated systems. Without the resolution of domain names into IP addresses the Internet is inaccessible for the general public. The Internet infrastructure should be prepared for future growth as the number of connected devices increases, as well as increasing volume of data traffic. IXPs play a vital role in improving the affordability, performance and reliability of the Internet.

Vulnerabilities in the technologies supporting industrial control systems

Cyber security protection framework can be adopted for identifying control system security protection measures and comparing them with existing security standards.Industrial Control System security Protection profile was developed by the National Institute of Standards and Technology. This framework provides a methodology for assessing the cyber security posture of control system which is designed to reduce the burden on the owners which reduce their respective risk. Risk= Threat * Vulnerability * consequence. The industries can make use of cyber security protection framework to secure the control systems against cyber-attacks.

Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data

Privacy refers to policies that protect the information contained within the voter registration database (VRD) against inappropriate access. The security of the VRD is necessary to ensure that the VRD properly performs its function as an accurate and complete list of registered voters. Security issues in VRDs is due to the following reasons. State VRDs contain personal information associated with registered voters, and such information must be protected against disclosures not permitted by law. The overall integrity of the VRD must be protected against unauthorized alterations (e.g., individual records being improperly added, deleted, or changed). The VRD system must be avail reliability in face of human, machine, or network failure is also an important dimension of system trustworthiness.

The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis

Mobile device threats are increasing on a daily basis. Cyber criminals are working on new techniques for getting through the security of the organizations by accessing everything from IP to individual customer information.They can cause damage, disrupt sensitive data and steal intellectual property.We cannot tell exactly what kind of threats will emerge next year orinfive years. These threats can beeven more dangerous than those of today. With the help of cameras and sensors, there is the possibility to avoid, physical threats, which might occur at the workplace or home.

Unauthorized access to devices that take an increasing role in people's daily lives

Cyber security makes headlines on a daily basis. Spam filters must be present. Authentication should be robust to make sure email is protected. Companies should also scan emails for potential threats. Unauthorized access to internet-monitored home security, traffic monitoring or CCTV systems can cause serious privacy, material, physical or emotional harm. Another important risk that is faced by the community is maintaining private data in devices that can be hacked by intruders and opens gate to cyber crimes. One such serious problem that threatens people's life is the recently hype BLUE WHALE game.

Dr.N.Sudha Bhuvaneswari