Defence Science Journal, Vol. 67, No. 4, July 2017, pp. 483-484, DOI : 10.14429/dsj.67.11542

OPINION

Cyberspace Security : An Overview for Beginners

Nitin Rai[*] and Shailesh R. Chansarkar[#]

[*]*Directorate of Cyber Security, DRDO HQ, Delhi - 110 011, India*
[#]*Centre for Artificial Intelligence and Robotics, Bengaluru - 560 093, India*
[*]*E-mail: nitinrai@hqr.drdo.in*

Internet is perhaps the only technology invented by mankind which has singly led to what is appearing to be the third revolution after the renaissance and the industrial revolution. The Internet, as of today, proposes to connect everything driven by the semiconductor, naming it off late, as the Internet-of-Things (IoT). It has over the years, connected the semiconductor driven systems and their human users, evolving the connected whole including the human user represented in that common whole, being called the cyberspace. This cyberspace consists of all the computing, processing, storage, printing, communicating, networking, etc. devices together with the large mass of human population using it.

The flowing time has integrated cyberspace into our lives like other technologies and utilities from the simplest to the complex. But do we understand the careful usage of it, so as to derive with confidence of safety and security, the comforts it provides. We all use utilities in the our daily lives like the utensils, knives, washing machines, refrigerators, televisions, phones, computers, etc. very commonly. Do we not use the knives in the kitchen for useful purposes even though we are ourselves vulnerable to being hurt by them? Do we not have power points in our homes to drive, televisions, microwave ovens, etc. even though small children in the house are vulnerable to putting their fingers into those fatal power points? Similar is the Internet which has woven us together into this revolutionary and yet vulnerable cyberspace. We need to learn its safe and secure usage.

Along with the evolution of the cyberspace, there has been phenomenal growth on its darker side which include the vulnerabilities that keep multiplying and acting as force multipliers for the illegal/harmful to dwell in and impact the cyberspace negatively. The dark side of the cyberspace is no different in impact in comparison to the real space or real world. It is also infested with crimes like cheating, extorsion, coercion, theft, etc. The ills of cyberspace are of both types, i.e. the ones which are human aided as well as the kind which are automated. The software technologies which are the tools for such dark activities are named as malware, virus, ransomware, spam, keylogger, worm, etc. The impacts of these dark activities are multifold. Users, might due to cyber theft, lose their passwords, credit card details and other identities. This could lead further to the denial of access for victims to their own digital assets or other symptoms also. For example, if a user's password for his email account is stolen, several issues can arise, like, the password might be changed and the user may not be able to use the email account again, the user's privacy of his email might get be lost and the user may not be aware of it, the user could get misrepresented using his email identity, etc. Several such possibilities lurk around in the cyberspace. There are malware, virus, worm, ransomware, etc. technologies which impact the cyberspace users like an epidemic, i.e. in large number widespread across the cyberspace geography. The latest one to impact on large scale was the ransomware named WannaCry. On 12th May 2017, this ransomware spread to unsupported and unpatched Windows systems, encrypting files and locking down systems until a bitcoin (internet based digital currency) ransom was paid. In other words, the users were required to pay ransom to unlock their own systems and the data resident on them! These kinds of impacts can manifest on targeted single individuals, individuals in large numbers, targeted cyberspace infrastructure, large cyberspace infrastructure or even a complete nation's cyberspace infrastructure and more.

Literature resulting from studies and research done in this area, articulates continuously increasing issues related to cyberspace security: *Privacy, integrity, accountability, availability, reliability, connectivity, recovery, liability, uncertainty, non-repudiation, confidentiality, and assurance*.

Perspectives of cyberspace security include variations from users, security administrators, developers, managers, entrepreneurs, etc.

Along with the growth of the darker side there has been significant contribution towards the positive. This too is multifold in terms of, technologies for prevention and protection from the malicious, legal regulations and provisions in the human world of users, and complementary documentations, guidelines, advisories etc., towards safe usage. This research and development towards secure and safe residence in cyberspace is called cyberspace security.

Several technologies have been developed and deployed over the decades and are being continuously improvised upon. Each of the technologies developed; address one or more issues related to cyberspace security mentioned earlier. Firewalls address the issue of privacy by providing access control to the user and infrastructural assets. Antivirus and anti-malware technologies address issues related to availability of infrastructure. Similar issues are addressed by intrusion

detection/prevention systems. Encryption technologies address the issues related to confidentiality and integrity. Technologies implementing digital signatures bring in non-repudiation and deal with issues related to accountability, liability, uncertainty, etc. There exists a large vendor base globally, which markets an ever evolving product catalogue of technologies for cyberspace security. The vendors generally place themselves in products development/sale, providing security services, or both.

Cyberspace security products are categorised broadly into; Network Security, Endpoint Security, Application Security, Web Security, Messaging Security, Data Security, Mobile Security, Cloud Security, Transaction Security, Industrial Security, IoT Security etc.

Cyberspace security services are not limited to, but include the following:

- Security operations and incident response
- Risk assessment and compliance auditing
- Access management
- Identity management
- Threat assessment
- Crisis management
- Total security management

Besides these technologies and services contributing to cyberspace security, there is an ever growing knowledge base incorporating artefacts like Standard Operating Procedures (SOPs) for usage of cyberspace infrastructure, guidelines for choosing a good password, emergency response advisories, etc. This knowledge base supports not only the large user base, but also developers of technologies which make cyberspace infrastructure more usable, for example; guidelines to secure programming. This kind of guidelines drives the developers towards developing such applications which are least vulnerable to automatic malicious attacks and exploitation. This knowledge base also includes certifications like the ISO certification towards secure/securely managed infrastructure.

The most important among the cyberspace security related assets for any country is the rules and regulations governing and defining what is legal and illegal in the cyberspace. This asset needs to also define the articles for cyberspace related crime. Thus it is up to the mankind to dwell wisely in the cyberspace.