Cyber Security: Situation and Challenges*

Lieutenant General Davinder Kumar, PVSM, VSM and Bar (Retd)**

Introduction

Information and Communication Technology (ICT) has ushered in globalization and with it a new security paradigm as well as a different way to conduct business. Its near instant reach and multiple connectivity, through powerful and responsive networks and systems, have not only made physical borders irrelevant, but have penetrated every aspect of human life. Its all pervasive nature and vast application range have relegated *Physical Security* by a number of steps on the security ladder. *Economic Security, Energy Security, Food Security, Water Security* and *Information Security* have achieved greater importance due to this globalization and the resultant interdependence as also the desire of all nations to give a better standard of life to its citizens.

The relative importance of these security layers can change depending on the nation's development index, priorities and perceptions. However, the criticality of Information Security has to be appreciated in the light of the fact that this is a common thread across all the security layers and hence, most critical. This is also more relevant as nations march from the agrarian/industrial era to the information/digital era.

Situation

Unfortunately, this common thread has also resulted in certain vulnerabilities in the digital domain as the dependency on networks and systems in general and internet in particular is growing exponentially. These vulnerabilities in cyberspace present a serious security challenge. According to a Norton study in 2011, 'threats

---

* Text of the paper presented by the author at the International Symposium conducted on 28-29 May 2012 at China Institute for International Strategic Studies (CIISS), Beijing, China on the subject "Cyber Security : China and the World" .

****Lieutenant General Davinder Kumar, PVSM, VSM & Bar (Retd)** is a former SO-in-C of the Indian Army. He recently retired as the Managing Director and CEO of Tata Advanced Systems Limited. He was nominated to represent USI at the above mentioned Symposium.

Journal of the United Service Institution of India, Vol. CXLI, No. 588, April-June 2012.

to cyberspace have increased diametrically in the past year affecting 431 million adult victims globally – or 14 adult victims per second and more than one million cyber crime victims per day.'

Cyberspace includes all networks and systems: telecommunications (mobile, cellular, wireless data services etc); process control systems like Integrated Control System (ICS); Programmable Logic Control (PLC); Supervisory Control and Data Acquisition (SCADA); data/contents in storage, transmission and processing; social networking in the digital world; Internet Protocol Television (IPTV) and the people who operate these. *Cyberspace is a* ***Global Common.*** It is man made and ever expanding. It is also a national asset. Here lies the biggest challenge, namely: what are the rules of sharing and demarcation of cyberspace?

ICT enables a host of business and government services to the citizens of a country. The Critical Information Infrastructure (CII) depends on it for its functioning, monitoring, maintenance and efficiency. In developed and some developing nations, ICT (cyberspace) has become the lifeline of critical infrastructure like energy, telecommunications, banking, stock exchanges, health services etc. Cyberspace has also become a critical area of Defence as also non-state players since it is an ideal resource for asymmetric warfare, the warfare of the 21st century. In cyberspace, a few state or non-state players can cause havoc through interference without the fear of attribution. Cyberspace is thus an ideal theatre of war supporting asymmetric warfare. It is due to this that today nearly 120 nations in the world are trying to develop technologies and capabilities to keep cyberspace safe as also have the ability to interfere with the cyberspace of the adversary. Here lies another challenge of defining Cyber War or Cyber Attack and the corresponding response expected.

Social Networking Platforms – a phenomenon that has gripped the entire world – have enabled people to come together across national boundaries and change the way they interact socially. It has become a medium for exchange of culture, values and governance. Its expanse, scale and easy reach have made it an ideal platform for Perception Management (an important part of information warfare) wherein a very large number of people can be mobilized for a cause as seen by recent international and national events *(Arab Spring, Jasmine, Wall Street Uprising, Anna*

Hazare's movement and so on). Currently, **Face Book** has 800 million users, which are expected to rise to one billion by August 2012. Tweets on **Twitter** grew from 500 K in 2007 to more than 4 billion in the Q1 of 2010, to over one billion tweets every week this year with a community of 225 million. *Here lies another challenge of the needs of national security vis a vis the individual's right of freedom of expression and privacy.*

There is an urgent need to secure cyberspace to ensure national security, proper governance and economic activities. We need to address the following:-

(a) What are the impediments to securing cyberspace?

(b) How can those impediments be overcome?

(c) What are the vulnerabilities and the associated threats to the National Information Infrastructure?

(d) How do we address the vulnerabilities linked to those threats in a timely, reliable and sustainable manner?

(e) How do we have a system in place which monitors the vulnerabilities and negates the associated threats in a dynamic and proactive manner?

No single individual, organization or a nation can find the answers to these issues and the continuously evolving problems of Cyber Security. A concerted and collaborative effort is needed both at the national and international levels to manage the situation and provide solutions. We need a concurrent 'Top Down' and 'Bottom Up' approach which should cater for a nation's security concerns in an acceptable international regime. This is a tall order as no nation will be willing to share its vulnerabilities and strengths. One hopes that continued discussion and awareness would foster more transparency and trust to appreciate each others' concerns and address the same in a more pragmatic manner.

Define, Identify and Recognize the Threat

Over the last decade, the world's understanding of cyber security has irrevocably shifted. Where once cyber crimes were seen as the domain of mischief making, basement dwelling loners, cyber attacks have now been recognized as the complex, pervasive threat that they really are.

As the secretive cyber world continues to mature, the internet has become the scene of a covert international battleground, the likes of which has never been seen before. On the new digital frontline, the boundaries between the military, civilians and the corporate worlds have blurred as governments, companies and individuals ranging from politically inspired "hacvtivists" to black market freelancers vie for the upper hand to pursue their agendas. Cyber incursions are no longer designed only to shut down websites and steal digital data; they are now capable of affecting real, physical infrastructure – an ominous precursor for the future.

Cyber Security is a generic term which has a number of constituents like: *Cyber Attack, Cyber Espionage, Cyber Terrorism, Cyber War, Cyber Forensics, Cyber Soldier, Cyber Mercenary* and so on. It has varied players vis Individual Player (Hacker), Hactivisits (Loosely organized group of hackers), *cyber criminals, cyber terrorists, non-state actors and the state.* The targets could again be individuals, organizations or the nation state. There is an urgent need to clearly define these terminologies which are the standard definitions acceptable internationally. Such an action will facilitate clear identification of threats and the corresponding responses including the associated Legal and Regulatory Framework.

Cyber Security Challenges. These are :-

(a) Coordination and cooperation between different stake holders both at the national and international levels.

(b) Reluctance to report cyber incidences. Hence, increased risk due to their invisibility and silence.

(c) Lack of awareness and respect for security. Security has to be seen as integral to governance and not a technical activity. Security has to be 'built in' and not 'bolted on'.

(d) Protection of a nation's CII is a major challenge since a bulk of it is privately owned. Yet, security and safety is seen as a Government responsibility with attendant reluctance on the part of private sector to invest.

(e) **ICT Global Supply Chain.** This is a major security concern both at the national and global levels. Given the increased dependence on global ICT products, especially in

critical sectors and the growing realization of cyber risks, countries are doubting the integrity of these products fearing that adversaries may introduce malicious codes/functions to do surreptitious surveillance, disrupt services or at worst paralyze a nation by eroding the functionality of its Critical Information Infrastructure (CII). Alleviating such doubts and fears to continue benefiting from global ICT supply chain, is one of the biggest challenges faced by the world in cyber security domain.

(f) **Poor Awareness and Education.** Another important challenge requiring special effort is to improve awareness and education about cyber security threats and need to follow best practices across different levels – from school children to housewives to government officials and management and corporate world. (It has been said that 80 per cent of the threats can be negated through following best practices). Adding to the problem is the non serious and reactive approach towards security as ingrained by a nation's culture. Many cyber threats can be mitigated if individuals are aware and vigilant.

(g) **Physical Provenance.** (The history of ownership of an object especially when documented or authenticated; like traceability in aerospace) of ICT components particularly in the process control systems.

(h) Absence of International and National Doctrines for Cyber Security and the associated Cyber security policies. The objects of such a doctrine should be :-

(i) To devise ways of eliminating threats and not just to identify defensive measures.

(ii) To clearly specify role, responsibilities and accountability regarding security of ICT components from producers to customers.

(iii) To codify normative behaviour in cyberspace and should identify cyber attacks and abuses as crimes or national security issues.

(iv) To include both policy and technical issues.

(v) To clearly state the response that a particular cyber incident would get.

(j) Understanding and addressing human behaviour is essential to building genuine security culture. It is a major challenge. There are also the related issues of the availability of requisite skill sets as also the equation between the collective right to security and the privacy of individuals.

(k) A dedicated organization for cyber security with single point responsibility and accountability.

(l) Cyber security standards need to be laid down in order to neutralise potential threats.

Weaponisation of Cyberspace. ICT has made asymmetric warfare more potent. There is a premium in attacking first due to the very speed of the attack. Besides, offence is a much cheaper option as the attacker has to exploit one vulnerability while the defender must monitor and protect the entire network/system. Today over 120 nations are developing offensive cyber capabilities. The challenge is to stop or regulate this through generating trust and confidence.

The Imperatives

Cyber Security is a global problem that has to be addressed globally through collaboration and co-operation by all countries. No government can fight cyber crime or secure its cyberspace in isolation. Cyber security is not a technical problem which can be solved; it is a risk to be managed by combination of defensive measures, astute analysis, information warfare and traditional diplomacy. It will always remain a work in progress as the threat is varied and dynamic. Fully secure cyberspace is a utopia!

There is an urgent need to have internationally acceptable legal norms regarding territorial jurisdiction, sovereign responsibility and use of force, investigation and prosecution of cyber crimes; data preservation and so on for dealing with cyber crimes. Globally acceptable norms for dealing with cyber incidents and transnational efforts for effective information sharing will help in securing the cyberspace.

Protection of CII will remain top national priority. Development of industry standards and sharing of best practices will better

equip organizations to respond to evolving and perennial threats. People, organizations and governments should be forthcoming to share cyber incidents. Emphasis also needs to be given to develop secure products, services and processes. A liability clause in the supply chain as in aerospace and nuclear fields will enhance the confidence of the industry.

Security must be prioritized as an embedded and integral function in every development. An impetus needs to be given for creating awareness and development of necessary skills. Cyberspace cannot remain safe unless its users are aware, vigilant and have the necessary skill sets to recognize and respond to cyber incidents.

Conclusion

In this Information Age, cyberspace is critical to meet the requirements of an individual, organization, nation and the world. We need to ensure that cyber security requirements or initiatives of any entity should not hamper the growth and availability of the cyberspace. We need to create awareness amongst the users about cyber security and ensure availability of requisite skill sets. While the security of the National Information Infrastructure would remain the top priority of any nation, there is an urgent requirement of international co-operation and collaboration for a legal and policy framework; defining terms like cyber crime, cyber attack and so on; laying down rules for sovereignty and jurisdiction in cyberspace. We need to ensure that cyberspace - the biggest Global Common – remains a driver of economic prosperity of nations and a platform where people from all nations can safely interact and exchange goods and services. Four Common Themes which emerge for ensuring cyber security are:-

(a) A coordinated and collaborative approach is needed.

(b) Metrics (Standards for measurement by which efficiency, progress, or quality of a plan, process or product can be assessed) for security are enablers and must be developed.

(c) An effective legal and policy framework for cyber security must be created.

(d) The human dimension of security must be addressed.