INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

CYBER SPACE – ISSUES AND CHALLENGES

*Piyush Patel

ABSTRACT

The Cyber space is borderless and actions in the cyber space can be anonymous. These features are being exploited by adversaries for perpetration of crime in the cyber space. The scale and sophistication of the crimes committed in the cyber space is continually increasing thereby affecting the citizens, business and Government. As the quantity and value of electronic information have increased, so to have the business models and efforts of criminals and other adversaries who have embraced the cyber space as a more convenient and profitable way of carrying out their activities anonymously. This paper will analyse cyber space issues and challenges in the digital world.

INTRODUCTION

Today adversaries are producing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyse and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness.[1837]

Malicious use of information technology can easily be concealed. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of state conflict. The source of these threats includes non-state actors such as criminals and, potentially, terrorists as well as States themselves. Cyber aggressors utilize various vulnerabilities in cyberspace to commit illegal acts on the internet. They exploit the

*2nd Year, LL.B, Faculty of Law, University of Lucknow, UP.

[1837] XII five-year plan (2012-2017) on Information technology sector, Report of Sub-Group on Cyber Security, Government of India Ministry of Communications & Information Technology Department of Information Technology

weaknesses in software and hardware structure by use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defenses of protected computer systems and interfering with their functioning. Identity theft is also common nowadays. The scope and nature of threats and vulnerabilities is multiplying with every passing minute[1838]. Major challenges in cyber space can thus be categorized as cyber warfare, cybercrime, cyber terrorism, and cyber espionage and protection of critical information infrastructure.

Key considerations for securing cyber space are as follows:-

- ✓ The security of cyber space is not an optional issue but an imperative need in view of its impact on national security, public safety and economic well-being.
- ✓ Cyber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.
- ✓ Effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations.
- ✓ There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.
- ✓ Security is all about what people, process and technology and as such there is a clear need for focusing on people and processes while attempting to use the best available technological solutions, which otherwise could prove ineffective[1839].Use of adequately trained and qualified manpower along with suitable incentives for effective results in a highly specialized field of cyber security.

Cyber Warfare

The issue whether cyber-attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated. Multilateral discussions are veering around to debating whether there should be rules of behavior for state actors in cyberspace. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution. There is, however, ongoing debate between those who believe that cyber warfare is over-hyped and those who believe that the world is heading towards a cyber-Armageddon. Both sides have

[1838] National Cyber Security Policy, draft v1.0
[1839] National Cyber Security Policy, draft v1.0

valid arguments, but even as that debate continues, cyber warfare as a construct has become inevitable because the number of countries that are setting up cyber commands is steadily growing. These commands have been accompanied by efforts at developing applicable military doctrines. There is, therefore, a pressing need to think about norms for cyber warfare, whether the laws of armed conflict (LOAC) can be adapted to cyber warfare, and how principles like proportionality and neutrality play out in the cyber domain.

There have also been cases of offensive action such as reports of shutting down of power systems. Such attacks on critical infrastructure either singly or in multiples are of serious concern, especially with respect to national security. The draft National Cyber Security Policy (NCSP) mainly covers defensive and response measures and makes no mention of the need to develop offensive capacity. This is a must if we are to ensure capability for self-defence granted under Article 51 of the UN Charter. This leads to the question: what is cyber warfare? In the absence of a formal definition of cyber warfare, we may define it as "actions by a nation-state or its proxies to penetrate another nation's computers or networks for the purposes of espionage, causing damage or disruption". These hostile actions against a computer system or NW can take two forms: cyber exploitation and cyber-attacks. Cyber exploitation is in a manner nondestructive and includes espionage. It is usually clandestine and is conducted with the smallest possible intervention that allows extraction of the information sought. It does not seek to disturb the normal functioning of a computer system or NW. The best cyber exploitation is one that a user never notices. These are silent and ongoing, and as mentioned earlier, have shown an upward trend. Cyber-attacks on the other hand are destructive in nature. These are deliberate acts of vandalism or sabotage – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy an adversary's computer systems or NWs or the information and programs resident in or transiting these systems or NWs. Actors in both types of activities cover a wide range, as mentioned earlier. Of these, nation states and their proxies are of the greatest concern. For easier understanding, the domains of cyber warfare may broadly be classified as:

1. Espionage i.e. Intelligence gathering and data theft. Examples of this were Titan Rain and Moonlight Maze. These activities could be by criminals, terrorists or nations as part of normal information gathering or security monitoring.
2. Vandalism i.e. defacing web pages or use DDOS to take them down. Such actions were evident in Estonia or Georgia.
3. Sabotage i.e. this has the most serious implications and includes DDOS, destruction of data, insertion of malware and logic bombs. It also encompasses actions in war such as those taken for preparation of the battlefield.[1840]

[1840] IDSA Task Force Report on "India's Cyber Security Challenge", Institute for Defense Studies and Analysis, Government of India, March 2012, Delhi, pg. no-31

Fifth Domain of Warfare

The cyber warfare is that which is practiced mainly by nation states or their proxies. The potency of this threat has compelled almost every country to develop capabilities in the cyber domain, as is the case for land, air, sea and space. Now it is essential requirement for the nation states to possesse varying degrees of cyber-attack capabilities. In addition, an unknown number of extremist groups and non-state actors have developed or acquired cyber weapons. Some commercially available products are flexible enough to be classified as dual-purpose – security testing tools and weapons of attack. Thus some organisations have or are developing cyber weapons and cloaking them as security testing tools. All this is classified information and each nation works on its own. An assessment of cyber warfare threat matrix by the USA, which covered over 175 countries and organisations, made a watchlist in which the top ten in order of priority were: China; Russian business NW; Iran; Russia tied with France; extremist/terrorist groups; Israel; North Korea; Japan; Turkey; and Pakistan. India on its growth path is vulnerable. Located in an unstable region where the larger neighbours possess this capacity, it is logical to assume that the country is under serious threat and constant attack. The impact on national security is thus serious and such that all institutions and organs of the state must jointly work tocounter this challenge. In order to understand the challenge, the following issues need to be addressed.

- ✓ Coordination: It is appreciated that in keeping with current needs, the Defence forces, DRDO, NTRO, CERT-In, RAW, IB, C-DAC, Ministries, NIC, NASSCOM, private industry et al. have to work in concert. The impact of this on every aspect of electronic media requires a coordinated and integrated approach. Given its all-encompassing nature, it also follows that control of all cyber and IW activities at the national level must fall under the purview of the NSC and controlled by its Secretariat ie the NSCS. Within this lead agencies for executing offensive cyber operations inter alia could be the NTRO, CIDS and the DRDO64.
- ✓ Defining Objectives and Doctrine: Application of such measures must be in accordance with clearly defined objectives that would be in keeping with customary international law and practice. The primary objective would be to garner knowledge to find how systems are breached and thus provide the ability for defensive measures to be developed and put in place. There is a further argument that it must be visible as an armor of self-defense so as to deter an attack. While this capability will be ambiguous, subtle signals and clear definition of objectives will lend credibility. Moral arguments stand thin in the face of realities. There is therefore a need to lay down the objectives and include them in the draft NCSP or issue a doctrine in this regard.

- ✓ Proactive Cyber Defence: This comprises actions taken in anticipation to prevent an attack against computers and NWs. As opposed to the current practice of passive defence, it provides a via media between purely offensive and defensive action: interdicting and disrupting an attack, or an adversary's preparation to attack, either pre-emptively or in self-defence. Proactive cyber defence will most often require operationalising upstream security mechanisms of the telecommunications or Internet providers. The most compelling reasons for a proactive defence can be couched in terms of cost and choice. Decision-makers will have few choices after an impact, and all of them are costly to start with. Proactive defence is thus the key to mitigating operational risk. The USA had set up a Proactive Pre-emptive Operations Group (P2OG) in 2002. Such actions thus find international acceptability65.
- ✓ Critical Infrastructure: There is a need to prioritise and protect critical infrastructure. In the USA 18 sectors have been identified. In India's case, the sectors of power, water supply, communications, transportation, defence and finance are vital constituents of national security. These need to be defined and suitable protection measures ensured as laid down in the IT Act. Steps to guard against threats, i.e. destructive actions or cyber exploitation will constitute a basis for research on offensive action. The electric power system merits top priority. While the risk of an attack can be reduced, it would be unrealistic to assume that an attack can be prevented. This leads to the conclusion that containment, isolation, minimizing the impact, backup systems and reactivation are areas of capacity building. The debate on which agency will undertake this in India rages and begs immediate resolution. As critical infrastructure spans both the public and private domains, the organization to ensure its protection has to be in the public realm and, in a manner, accountable.
- ✓ Legal Provisions: The IT Act of 2008 covers all actions in this domain. Sections 69, 69A and 69B contain provisions for intercepting, monitoring or blocking traffic where, amongst other reasons, there is a threat to national security. Section 70A covers protection of critical infrastructure. There is a need to work within these provisions The cyber realm, with scope of non-attributable actions as also ease of deniability, provides immense scope for exploitation. The fact that there are no international cyber laws or treaties at present is also used to advantage. Offensive cyber operations by their very nature have to remain in the grey realm and restricted. Each nation would thus determine the structure best suited to its needs. However, the necessity to clearly enunciate such measures or self-defence actions in a doctrine as also the NCSP is essential for steps in this regard; it also acts as an element for deterrence. The emphasis must remain on protecting NWs, systems and users.

Meeting the Cyber Warfare Challenge

Cyber warfare encompasses government and public and private domains. As clarified earlier, this must be coordinated by the NSCS. In the USA it comes directly under the White House. Thus the need to create a Directorate or Special Wing in the NSCS for this. It would oversee and coordinate both defensive and offensive cyber operations. There is also a requirement for intimate involvement of the private sector, as they are equal, if not larger, stakeholders. Regular meetings must be held and, if needed, working groups created. Current organizations which could be tasked to take on the cyber warfare challenge include the NTRO, HQ IDS, DRDO, RAW and IB. Representatives of CERT, NASSCOM, etc. will invariably be involved. Each would have to function under guidelines and through proxies[1841].

- ✓ Raising of Cyber Command: While cyber warfare is ongoing activity during peacetime, there is a dire need to develop this capacity for a warlike situation. Cyber warfare in a manner is NCW and will form an essential part of preparation of the battlefield in any future conflict. Such attacks may also precede the kinetic war. Building this capability will take time and must remain covert and ambiguous. It could also form part of the strategic deception process. This should be the responsibility of the Armed Forces (HQ IDS) along with the DRDO and other experts. Detailed discussions and consultations in this regard require to be initiated. India must raise a Cyber Command. This will comprise not only the three services but personnel from the DRDO and scientific and technological community. It could work with the space command because many aspects overlap and would economize on resources. It will oversee all activities undertaken during peacetime, as also plan for offensive cyber operations as required, to include preparation of the battlefield. It must work in close concert with the NTRO. To determine the structure it would be prudent to study the mission and objectives of USCYBERCOM as a guide. USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: "direct the operations and defense of specified Department of Defense information NWs and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." The Command is charged with pulling together existing cyberspace resources, creating synergy and synchronizing war-fighting effects to defend the information security[1842] environment. It comes under the Strategic Command, which also has the Space Command as a constituent. A similar structure for India could be considered, especially as the US has evolved

[1841] IDSA Task Force Report on "India's Cyber Security Challenge", *Institute for Defense Studies and Analysis, Government of India*, March 2012, Delhi, pg. no-34
[1842] Ibid.

its structure based on experience and also because it functions as an open democracy. India already has the Strategic Forces Command, which could be augmented with both Space and Cyberspace Wings. These may be of smaller size to start with, and will develop in accordance with threats and needs. Each service has its own requirements. The structure therefore has to be need-based and flexible. The various elements of this could be:

i. Army, Navy and Air Force CERTs : These would monitor traffic, disseminate information, ensure remedial measures to ensure ongoing security to NWs and systems. They would also in a manner be charged with protection of critical infrastructure of each service, i.e. communication backbone, power systems, high-priority NWs, et al. The structure thus envisages a Defence CERT which works in concert with each service CERT.

ii. Intelligence and information operations: A Defence Intelligence Agency exists under HQ IDS. Its cyber and information operations elements could work with this command. Intelligence gathering is an accepted reality and cyberspace possibly provides the best scope for this as also information operations.

iii. Defence communication NWs: Each service has its special requirement sand own communication directorates. Joint operations, strategic communications as also high-security NWs need to be coordinated under HQ IDS and the proposed Cyber Command.

iv. Cyber operations which are required for preparation of the battlefield. This again would be a tri-service organisation, with additional experts from the DRDO or any other such institution. This would include R&D.

Cyber Crime

The increasing online users has proved a great hunting ground for cyber criminals, with losses due to such illegal cyber activities being in billions of dollars globally. While countries are reporting huge losses due to cybercrimes, as well as threats to enterprises and critical information infrastructure (CII), there are reports coming out of those relating to cyber espionage. Even though the Information Technology Act (IT Act) 2000 confers extraterritorial jurisdiction on Indian courts and empowers them to take cognizance of offences committed outside India even by foreign nationals provided "that such offence involves a computer, computer system or computer network located in India", this has so far existed only on black and white. Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere. Companies attribute this to the primacy placed on information assurance in the outsourcing business. Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such

as the establishment of the Data Security Council of India (DSCI) and the National Skills Registry. The Indian government has also aided these initiatives in a variety of ways, including deputing a senior police officer to NASSCOM to work on cyber security issues, keeping the needs of the outsourcing industry in mind. That said, cyberspace is increasingly being used for various criminal activities and different types of cybercrimes, causing huge financial losses to both businesses and individuals. Organized crime mafia have been drawn to cyberspace, and this is being reflected in cybercrimes gradually shifting from random attacks to direct (targeted) attacks.

A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets. The vast amounts of money lubricating this ecosystem is leading to increased sophistication of malicious codes such as worms and trojans. The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars.

Cyber terrorism

Cyberspace has been used as a channel for planning and implementing terrorist attacks, for satisfying their terrorists political and social objectives and creating fear in minds of people.[1843] Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes.

Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at reast cause enough harm to generate fear, Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact. Attacks that disrupt non essential services or that are mainly a costly nuisance would not. This is one of the most comprehensive definitions of cyber terrorism. But even this has a limitation. It states that for an attack to qualify as a cyber attack it should lead to violence. This is more conventional. Terrorist may direct an attack only to disrupt key services, if they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous.

[1843] Siddiqui, M. Zakaria, "Cyber Tenorism: Global Perspective." The Indian Journal of Criminology and Criminalistics, Vol. XXII, No.2 May-Aug. 2001

The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities, especially in the aftermath of the terrorist attack in Mumbai in November 2008. Parliament passed amendments to the IT Act, with added emphasis on cyber terrorism and cybercrime, with a number of amendments to existing sections and the addition of new sections, taking into account these threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements[1844]. While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyber terrorism both in terms of methods and end goals.

Cyber terrorist prefer using the cyber attack methods because of many advantages for it.[1845]

a) It is Cheaper than traditional methods.

b) The action is very Difficult to be tracked.

c) They can hide their personalities and location.

d) There are no physical barriers or check points to cross.

e) They can do it remotely from anywhere in the world.

f) They can use this method to attack a big number of targets.

g) They can affect a large number of people.

Efforts of combating cyber terrorism.

The Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism. They are helping all the member countries and training their personnel. The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. There is need to establish and maintain international standards of accountability. States that have sovereign rights also have sovereign responsibilities, including the responsibility to

[1844] Crabtree, S. (1996) Cyberspace: a Terrorist Frontier? Insight on the News, 12 (31)
[1845] Prof. Soumen Ganguly, "Impact of Cyber terrorism in digital world", International Journal of Computer Science and Information Technology & Security (IJCSITS).Vol.1, No. 1, October 2011

combat terrorism. The international community has developed a compelling body of international obligations relating to counterterrorism. Twelve universal conventions and protocols in force against terrorism have been developed under the auspices of the United Nations as well as various U.N. Security Council Resolutions related to combating terror. These include UNSCR 1373, which imposes binding obligations on all states to suppress and prevent terrorist financing, improve their border controls, enhance information sharing and law enforcement cooperation, suppress the recruitment of terrorists, and deny them sanctuary. The Group of Eight (G-8) along with other multilateral and regional bodies also have been instrumental in developing landmark counterterrorism standards and best practices that have been adopted by international standard-setting organizations.[1846]

Cyber Espionage

Cyber espionage refers to state-sponsored theft of industrial and defense secrets and/or intellectual property. The state sponsored cyber espionage poses a serious threat to the economic and national security. Military secrets and valuable corporate intellectual property undermine the long-term competitiveness of the targeted countries.[1847]

One particularly insidious form of cyber espionage is known as an advanced persistent threat (APT). APTs are highly targeted malware-based attacks with several distinguishing features. First, as their name suggests, APTs are often advanced. In many cases, they utilize the full spectrum of computer intrusion technologies and techniques and combine multiple attack methodologies and tools in order to reach and compromise their target. Second, APTs are persistent. APT operators seek long-term access to their targets, with attack objectives generally extending beyond immediate financial gain. In order to maintain long term access to targets, APTs generally operate stealthily for as long as possible. Finally, APTs rely on skilled, motivated, organized and well-funded operators to coordinate and execute attacks. The substantial resources required to operate APTs generally makes them a tool of nation-states. At their essence, APTs are computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the 'art of manipulation,' in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information[1848]. Instances of such a cyber-threat are becoming quite common these days, as we see regular reports related to thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and NWs of

[1846] HLS, 2002. National Strategy for Homeland Security. Office of Homeland Security. July 2002
[1847] Contreras, et al., Faculty of Law University of Copenhagen, American University Law Review, (2013) pg. 114-115
[1848] Melanie J. Teplinsky, "Fiddling on the Roof: Recent Developments in Cybersecurity" American University Business Law Review, Volume 2, Issue 2 pg. 255-256 (2013)

both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. Companies are also reluctant to disclose any attacks and exfiltration of data, both because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public. As far as infiltration of government NWs and computers is concerned, cyber espionage has all but made the Official Secrets Act, 1923 redundant, with even the computers in the Prime Minister's Office being accessed, according to reports. The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult; governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive NWs, and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exfiltrated.

Protection of Critical Information Infrastructure

PPP in National Security

National security has traditionally been the sole responsibility of governments. But as the world has moved into the information age, with increased dependence on information infrastructure for production and delivery of products and services, the new responsibility of securing the critical information infrastructure (CII) against the rising number of cyber-attacks has come within the ambit of national security.

Information sharing and Coordination

While CERT-In is doing an excellent job in the government sector, the same needs to be replicated for the private sector through establishment of Security Information Sharing and Analysis Centres within each of the identified private sectors, that coordinate with CERT-In and/or National Nodal Centre that may be created. Information sharing between government-to-private and private-to-private should be promoted. In this context it is pertinent to study the effectiveness of information sharing programmes elsewhere in the world, especially in the United States, which has put in place voluntary approach based

on information sharing and PPP at the centre of cyber security policy[1849]. The difficulties they have encountered include private entities' inability to share information because of liability, anti-trust, and business competition risks. From the government side, difficulties of sharing classified information with the private sector have been reported. It seems that many of the information-sharing activities will require even legal changes to make this programme work. It is recognised throughout the world that the private sector follows high standards of security compared to its counterparts in the public sector, and that the latter can learn from the practices in the private sector. There should be appropriate mechanisms for the public sector to use such security practices as are followed in the private sector, for enhancing the cyber security posture and preparedness of the public sector infrastructure. Appropriate processes and structures need to be established to make this happen in our own environment. There should be a National Command and Control Centre, which should be responsible for coordinating cyber security-related activities at the national level for both the public and private sectors and also assign roles and responsibilities.

Innovation in Regulatory and Security Approach

The government can intervene in protection of CII by the private sector by enacting stringent regulations. Though regulations are necessary they should not add cost without necessarily improving security of CII. Too much of government intervention through regulations can also undermine business innovation. In addition to enacting promotional legal framework for securing CII, the government must also create incentives for industry to invest in security of CII beyond what is necessitated by companies' business plans. Examples of such incentives could be tax deductions and rebates on security investments, lower cost loans for SMEs that implement best security practices, reduced liability for improved security, recognition, etc. Information security is considered as one of the biggest inhibitors to business innovation. The executives of the companies have admitting that their organisations have "occasionally" or "often" backed away from innovative business opportunities because of information security concerns.

Proactive threat and vulnerability Management

The success of a security programme lies in the ability of an organisation to swiftly respond to security threats and attacks. This requires more proactive delivery of security intelligence. CERT-In may like to partner with the private sector for a focused effort to create enablers for increasing interactivity with security organisations of critical sectors

[1849] Ibid.

for sharing the research findings and information. Government should enhance interactivity of security organisations with national cyber security machinery, with active participation of the private sector. There is an urgent need to revitalise security in the critical infrastructure sectors as they become obvious and lucrative targets of security threats. This requires significant resources and efforts. For example, SCADA systems may require a sustained nationwide security analysis centre. A programme is required to create an inventory of information assets. The sectors may not be in a position to fund the investment. For proactive defence, the government needs to intervene to fund implementation of security practices in these sectors. Government should initiate a special drive of implementing practices in the critical infrastructure sectors and provide necessary budgetary support for such implementation.

Security in IT Supply Chain

IT supply chain, in its reach and characteristics, reflects a high level of globalization. In fact, that has been one reason for the success and continuous growth of the Internet. Innovations of technology, products and services, with components such as chips, tool sets, operating systems, databases, applications, and so on have ensured that no single country can claim to innovate, design, test, manufacture, operate and maintain hardware and software products and services. A veritable global chain has emerged – the ICT Supply Chain. This poses a critical challenge for obtaining assurance over the security of the product and services being outsourced to, and procured from global technology[1850] providers. With increased dependency on cyberspace, increased concern about cyber threats, and increased appreciation of the globalisation of the development, manufacture, and maintenance of ICT systems, fears have grown that adversaries will taint the supply chain to engage in espionage. They might introduce hidden malware, and change functionality of products and services with a view to give their own countries advantages that are difficult to gain otherwise. For example, a service could be disrupted at critical junctures, or kill switches may be planted to disable a CII organisation.

Participating in International Efforts

The Government of India should take leadership in international efforts and cooperation for cyber security as many cyber attacks on CII originate from foreign countries. For example, India could lead an international co-operation that makes a nation responsible for the actions in cyberspace of individuals who are resident in its territory. A good example of similar effort is the Financial Action Task Force (FATF). FATF began as a

[1850] IDSA Task Force Report on "India's Cyber Security Challenge", Institute for Defense Studies and Analysis, Government of India, March 2012, Delhi, pg. no-42

group of nations opposed to money laundering. They established practices and rules for banks and for banking authorities to make money laundering more difficult. Nations that did not comply faced greater difficulty in participating in the global financial NWs – higher costs, longer delays, more impediments. A similar approach to nations that tolerate cyber crime could be to make it more difficult for them to connect to the global NW, or to have their national NWs face additional scrutiny and impediments. These constraints would not be foolproof but they would increase the cost to nations that act as sanctuaries and provide incentives for changed behaviour.[1851]

Cyber Privacy

Every person has a desire to keep a part of his life private. This is broad meaning of "Privacy". The area of life which one wants to keep away from the public gaze may relate to one's personality, one's name, one's private life, one's papers and the like. It is a privilege to live without unjustifiable impedance by general society in matters with which people in general is not really concerned.Right to Privacy like any other right is not absolute; disclosure of personal information is justified under certain circumstances Hence privacy, in simple terms, can be defined as the right to be left alone.[1852] Each and every person should have the right to control the amount of information about himself which he wishes to share.

The Hon'ble Supreme Court of India in R. Rajagopal v. State of T.N.[1853] held the right to privacy as an integral part of the fundamental right to life under Article 21 of The Constitution of India. The right to privacy is a right to be let alone. None can publish anything concerning the above matters without his consent, whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.

CONCLUSION

Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. Their effects carry significant risk for public safety, the security of

[1851] James Andrew Lewis, The Cyber War Has Not Begun, Center for Strategic & International Studies, March 2010
[1852] Warren and Brandeis, The Right to Privacy, Harvard Law Review,(1890) Vol. 4, Issue 5 , pp. 193-220
[1853] R. Rajagopal v. State of T.N, (1994) 6 SCC 63

nations and the stability of the globally linked international community as a whole as a faceless organisation, the internet seems to offer both secrecy and security something which may be hard to come across in real life. It seems almost inconceivable that our privacy could be infringed in any way, much less by the very agencies which purport to protect us.