A Case for National Cyber Security Strategy

Dr. Muktesh Chander, IPS*

The Indian Police Journal
@BPRD, MHA
BPRD Publication
www.bprd.gov.in

"I dream of Digital India where cyber security becomes integral part of national security" [1]

"The world has left the Cold War behind only to enter into a Code War" [2]

Abstract

In the digital era, almost all human activities have been impacted by computers and Internet. The growth of cyber crimes has threatened these activities. Any cyber attack on critical information infrastructure can have a debilitating effect on our national security, economy, public health or safety. Cyber security is now an integral and important part of nation security strategy. When several countries are seriously perusing cyber weaponization programs, it is pertinent to formulate a well defined and articulated National Cyber Security Strategy.

Keywords:

Critical Information Infrastructure, Cyber crime, Cyber espionage, Social media attacks, Cyber weaponization, Cyber Westphalia, Cyber deterrence, Cyber resilience.

1. Introduction

Increasing use of computers, computer networks, and information & communication technology (ICT) has resulted in a huge amount of vital information being exchanged, stored and processed on computers. This is not only true for individuals, various types of organizations and companies but also for governments and their institutions. This digital information needs to be accessed from various computers through various kinds of networks by various users such as citizens, customers, employees, vendors, business associates, governments, etc. The confidentiality, availability and integrity of this information are crucial for nations to effectively run their E-Commerce and E-Governance models. Digital economy is now dependent on global network of economic and social activities that are enabled by increasing computerisation of all aspects of human activities. As India is digitally integrating with global economies and societies, her reliance on information systems and networks, that are complex, interconnected and interdependent, is increasing exponentially. These interconnected networks and systems, widely acknowledged as "Critical Information Infrastructure (CII), are those facilities, systems or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of our country. Therefore protection of these CII's is of strategic importance to our national security. We have seen terrorism and violence as a part of proxy war for a long time. After land, sea, air and space, warfare has entered the fifth domain of cyberspace[3]. Digital

Author Intro:

* DGP, Goa

[1] Shri Narendra Modi, Hon'ble Prime Minister of India, at the inauguration of 'Digital India Week', 2015.

[2] Alec Ross, "Weaponisation of Code", The Industries of Future, Simon & Schuster Paperbacks, New York, Page 121.

[3] The Economist, "War in the Fifth Domain", The Economist, 1st July 2010, available at http://www.economist.com/node/16478792 (accessed 6th June 2017).

India will be vulnerable to cyber attacks if a well articulated cyber security strategy, as an integral part of national security, is not defined and implemented.

2. Rise of Cyber Crimes

According to National Crime Records Bureau 12317 cases of cyber crimes were registered under Information Technology Act in 2016. This figure may not reveal the true picture of the actual prevalence of cyber crimes due to various obvious reasons. Cyber crimes are increasing world over and there is no reason for being complacent about the low official figures in India. Indian Computer Emergency Response Team handled 50362 cyber security breach incidents in 2016. More than 31664 Indian websites were defaced and about 1,00,20,947 'Bot' infected Indian systems were tracked. Cyber crimes cost India a whopping Rs. 24,630 crore in 2013 alone as criminals used sophisticated means, says a Delhi High Court-commissioned report[4]. Cyber crime has emerged as a serious global threat. In 2014, a group of hackers, calling themselves as "Guardians of Peace", stole about 100 tera bytes of confidential information from Sony Pictures Entertainment, some of which was leaked online. The group threatened to leak more information, forcing Sony to abandon its plans to release movie "The Interview". In one of the most dramatic bank robberies, hackers stole $81 million from Bangladesh Central Bank's account at the New York Federal Reserve by manipulating instructions to computers of Society for Worldwide Interbank Financial Telecommunication (SWIFT). In 2013, FBI took down international online illicit trade in drugs and other contrabands. Code named "Silk Road" was first modern darknet market, which operated using encrypted mail, virtual currencies and anonymous 'TOR' browsers. In 2016, in the first ever cyber attack using "Intenet of Things", hackers were able to bring down services of Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, Fox News as well as newspapers including the Guardian, the New York Times and the Wall Street Journal. The attackers used hundreds of thousands of internet-connected devices that had previously been infected with a malicious code that allowed them to cause an outage[5]. In 2016, cash worth 1.4 billion Yen was withdrawn, in less than three hours, from 14,000 ATMs in Japan, using fake credit cards created with data stolen from a South African bank. World Economic Forum, in its Global Risk Report, has indicated cyber attacks to be one of the risks with highest likelihood of occurrence and highest impact[6]. In view of global situation, official statistics, indicating low cyber crime incidents in India, should not make policy planners complacent. We need to learn lessons from our coastal security analogy, where existing vulnerabilities were all known but serious action started only after 26/11 Mumbai attack. As in the real world, we are also constantly engaged in low scale cyber war with our neighbours. This is evident by the hacking of Indian websites and the cyber espionage attempts from time to time. In the absence of an action plan, this conflict in cyber space is likely to escalate to more serious cyber attacks on our digital backbones.

---

4 Economic Times, "Cyber crimes alone cost India Rs 24,630 crore in 2013: Report", available at http://economictimes.indiatimes.com/tech/internet/cyber-crimes-alone-cost-india-rs-24630-crore-in-2013-report/articleshow/37892659.cms (accessed on 7th June 2017).

5 Reuters, "Cyber attacks disrupt PayPal, Twitter, other sites", available at http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME (accessed on 7th June 2017).

6 World Economic Forum, "The Global Risks Report 2016", available at http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf (accessed on 7th June 2017).

3. Cyber Attacks on CII

Coordinated and well planned cyber attacks on CII in several countries, using multiple cyber weapons, have already occurred and studied by experts. Estonia, one of the most wired societies in Europe and a pioneer in the implementation of E-governance, became victim of politically motivated large-scale cyber attacks on its CII in 2007. The attack lasted three weeks, affecting the Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three of the country's six big news organizations, two of the biggest banks and firms specializing in communications[7].The infection of Iran's nuclear power plant computers by "Stuxnet" malware has started a new cyber arms race and has created serious implications for the security of critical infrastructure worldwide[8]. Although targeted at Iran, Stuxnet spread to other countries including India. Ukrainian power companies experienced unscheduled power outages resulting from well coordinated and synchronized cyber attacks in 2015 and 2016. "Shamoon", a data-wiping malware, infected more than 30,000 computers of Saudi Arabia's firm Aramco in 2012[9]. Since 2004, South Korea has been facing series of cyber attacks from North Korean hackers[10]. A wave of cyber attacks, aimed at 27 American and South Korean government agencies and commercial web sites, temporarily jammed more than a third of them in 2009[11]. Recently WannaCry ransomware outbreak affected more than 230,000 computers in more than 150 countries. Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx, Deutsche Bahn and some U.S. critical infrastructure operators were hit. Over 48,000 attempts of WannaCry ransomware attack were detected in India also. Various hacker groups have been targeting our cyber space from time to time. Indian sectors of energy, transportation (air, surface, rail and water), banking and finance, telecommunication, defence, space, law enforcement, security and intelligence, sensitive government organisations, public health, water supply and disposal, critical manufacturing, e-governance have been identified as critical. There is a possibility of large scale cyber attacks on any of these. With this view in mind, a National Critical Information Infrastructure Protection Centre is now operational in India, deriving its mandate from Section 70 B of IT Act. The preparedness of our country, to deal with cyber terrorism, requires serious investment in cyber security technology, procedures and capacity building of professionals of all stake holder organizations.

4. Cyber Espionage

Industrial, economic and political espionage, using cyber means by individuals, state-sponsored actors and states themselves, are becoming a serious threat to the national security. In June 2013, Edward Snowden disclosed thousands of classified documents, revealing a global surveillance program by USA in association with some other countries, collectively called "Five Eyes". In 2012, "Flame", one of the most sophisticated malwares,

---

7 Ottis, R., "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" in Remenyi, Dan (Ed.), Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, UK, 30 June- 1 July, Academic Publishing Limited, pp. 163-168.

8 Collins, S. and McCombie, S., "Stuxnet: The Emergence of a New Cyber Weapon and its Implications", Journal of Policing, Intelligence and Counter Terrorism, Vol.7 Issue 1, pp.80-91.

9 Bronk, Christopher and Tikk-Ringas, Eneken, "Survival: Global Politics and Strategy", April–May 2013, Vol. 55, pp. 81-96.

10 Boo, Hyeong-wook, "An Assessment of North Korean Cyber Threats", available at http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf (accessed 6th June 2017).

11 Choe S-H and Markoff John, "Cyber-attacks Jam Government and Commercial Web Sites in U.S. and South Korea", The New York Times, available at http://www.nytimes.com/2009/07/09/technology/09cyber.html (accessed 6th June 2017).

specially designed for the purpose of cyber espionage, targeting several countries in Middle East, was discovered[12]. There are several reports indicating that India, Russia, USA, Sweden, South Korea and several other nations have been victim of cyber espionage to varying extent[13]. During February and March 2016, Kaspersky detected cyber espionage attacks from a hacker group named "Danti" which focused on Indian diplomatic entities using spear-phishing emails created in the names of several high-ranking Indian government officials[14]. In several attacks, hackers have used exploits which were known at least a year in advance and patches were available but not applied. The persistent cyber espionage efforts by foreign elements against sensitive Indian organizations call for a serious thinking. The game of espionage has entered its golden era and while playing it we have to not only defend but also score a goal.

5. Social Media Attacks

The power of social media, in influencing election results, was amply demonstrated during US presidential elections in 2016. A recent report has assessed Russian activities and intentions regarding US election[15]. This attempt, to tilt US election result in a particular direction, using the "Code war", involved hacking of emails from U.S. persons, political organizations and institutions. A significant role has been played by social media (particularly Facebook, Twitter and YouTube) in Arab Spring revolutions in Middle East[16]. The Islamic State of Iraq and Syria (ISIS) has the motive, means, and opportunity to acquire the personnel and codes necessary to launch devastating cyber campaigns. The Cyber-Jihadist organization already possesses a complex communication infrastructure to leverage attack[17]. Online radicalization of youths, all over the world, has drawn several of them to the terror world. Disinformation, using morphed images, fake videos and stories circulating on social media sites, have triggered serious violence and rioting in Assam, Muzaffar Nagar and several other places in India in recent past. In 2014, handler of a pro-ISIS Twitter account @ShamiWitness was arrested in Bengaluru after a foreign media broke this story. Burhan Muzaffar Wani, a Hizbul Mujahideen commander for South Kashmir, who died in an encounter with security forces, was using Twitter, YouTube and Facebook for glorifying Jihad, recruiting terrorist and online radicalization. Social networking sites are now one of the most fertile places for criminal activities. If monitored effectively, social networking sites can provide resourceful, economical and effective tactical and actionable

---

12 Chander, Muktesh, "Cyber Espionage: Lessons to be learnt from Snowden revelation", *Defence and Security Alert*, August 2014, pp. 26-27.

13 Thornburgh, Nathan, "Inside the Chinese Hack Attack", available at http://content.time.com/time/nation/article/0,8599,1098371,00.html (accessed 6th June 2017); IWM, "Tracking GhostNet: Investigating a Cyber Espionage Network", available at http://www.nartv.org/mirror/ghostnet.pdf (accessed 6th June 2017); McAfee, "Revealed: Operation Shady RAT", available at https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed 6th June 2017).

14 Kaspersky, "Danti and Co.: Cyber-espionage groups use a single vulnerability to target organisations around the world", available at http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Campaign/KESB_2013/Pdfs/25052016_press_release_danti-etc_eng_final.pdf (accessed on 8th June 2017).

15 ICA, "Assessing Russian Activities and Intentions in Recent US Elections", available at https://www.dni.gov/files/documents/ICA_2017_01.pdf (accessed on 6th June 2017).

16 Howard, Philip N. and Hussain, Muzammil N., "DEMOCRACY'S FOURTH WAVE?Digital Media and the Arab Spring", available at https://deepblue.lib.umich.edu/bitstream/handle/2027.42/117564/Democracy%27s+Fourth+Wave.pdf?sequence=1 (accessed on 10th June 2017).

17 ICIT, "The Anatomy of Cyber-Jihad", available at https://krypt3ia.files.wordpress.com/2016/06/icit-brief-the-anatomy-of-cyber-jihad1.pdf (accessed on 6th June 2017).

intelligence[18]. Monitoring of social media, for illegal activities and contents which have the potential of starting social unrest and large scale violence is still in nascent stages in India. Very few states have social media monitoring labs, trained staff and tools to carry out this important task of patrolling the cyber beat.

6. Cyber Weaponization

Stuxnet, Flame, Shamoon, Dist-track, Duqu and several other sophisticated malwares have already heralded the arrival of cyber weapons. This new high-tech arms race is different from nuclear weapons race because the resources required are cheap and available to anyone easily. Several nations have been developing, stockpiling and using such weapons. Anonymity, deniability and difficulty of attribution are encouraging this new arms race. Cyber war and cyber terrorism are no longer topics of debate but are a reality now. The use of ICTs in future conflicts between States is becoming more likely[19]. Tallinn Manual has defined several concepts including cyber war and cyber weapons[20]. Tallinn Manual 2.0 covers a full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of international law principles and regimes that regulate events in cyberspace[21]. The transition from Cold war to Code war has already occurred and it is time for every cyber nation to incorporate it in its cyber security strategy.

7. Westphalian Sovereignty in Cyber Space

Cyberspace is non-territorial, chaotic, unregulated and ungoverned. There is not even an international treaty on cyber crime in place. Application of Westphalian concepts of sovereignty in cyberspace has several different connotations. However, led by USA, there is a growing assertion by several nations that international laws apply to cyberspace and a state has a right of self-defense by retaliating in cyber as well as kinetic space, if it is under cyber attack[22]. At the UN level, a group of governmental experts agreed to an important set of recommendations on norms, rules, and principles of responsible behavior by states in cyberspace. The expert group has recognized that international law, including the principles of the law of state responsibility, fully applies to state behavior in cyberspace[23]. Several countries are now discussing the possibilities of regulating the conduct of nation states in cyberspace and evolution of some sort of cyber treaty for international cooperation. Cyber Westphalia and application of twin frameworks of *jus ad bellum* and *jus in bello* to cyber space are still in a state of flux, though evolving gradually. We should continue to participate and contribute to this evolving international process.

8. National Cyber Security Strategy

Liijf *et al*. have found three general goals for a national cyber strategy: (a) align the whole

[18] Fitsanaki, Joseph and Bolden, M.S., "Social Networking as a Paradigm Shift in Tactical Intelligence Collection", Mediterranean Council for Intelligence Studies Yearbook, Greece, pp. 28-40.

[19] UN, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed on 6th June 2017).

[20] "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University Press, New York, available at https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (accessed 6th June 2017).

[21] NATO, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", available at https://ccdcoe.org/research.html (accessed on 6th June 2017).

[22] Koh, Harold Hongju, "International Law in Cyberspace", Harvard International Law Journal Vol. 54, available at http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf (accessed on 6th June 2017).

[23] UN, "Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security", available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed on 6th June 2017).

government, (b) provide focus for public and private planning with established roles and responsibilities for all stake holders and (c) signal a nation's intent to external parties[24]. Several countries have now a well articulated cyber security strategy document, showing their commitment and approach to dealing with cyber threats. USA, UK, Australia, Canada, Estonia, France, Germany, Russia, Singapore and many others have made these documents public. India announced its National Cyber Security Policy in 2013. There after the Guidelines regarding Protection of National Critical Information Infrastructure were released[25]. To build a secure and resilient cyber space for citizens, businesses and Government and protection & resilience of Critical Information Infrastructure are two main objectives of this policy. These are being implemented by the designated agency under National Technical Research Organization[26]. Increasing use of computerised systems, networks and ICT, in governance as well as by digital society, has increased the vulnerability of our nation to cyber attacks. While we are creating Smart Cities and a Digital India, with focus on delivery of government services using mobile platform, we need to focus on the cyber security of our ICT backbones. Cyber attacks on CII, cyber espionage, malicious propaganda on social media, and online radicalization etc. pose a serious threat to our national security. Organised cyber criminal gangs, state-sponsored acts of cyber terrorism and cyber war can have far reaching crippling consequences. Cyber security has now become an integral part of national security and must find a dominant place in the overall national security strategy of India. We need not wait any longer to define and formally express it like other nations have done.

9. Cyber Deterrence

The conventional model of deterrence, which emerged during cold war and has continued in the nuclear era, is taking shape in cyberspace also. The concept of cyber deterrence builds upon the strategy of cyber defence by incorporating both the ability to retaliate and the will to retaliate towards the cyber attacker[27]. The peculiar nature of cyber attacks, coupled with difficulty in attribution, raises several challenges to cyber deterrence concept. Notwithstanding these challenges, there is convincing evidence to suggest that the US, UK, Russia, Iran, North Korea and China are taking extraordinary measures to build cyber armies for exploiting cyber vulnerabilities of adversary. Cyber space implies there will be attempts by countries to dominate it and emerge as cyber power. Australia's recent Cyber Security Strategy states that "Australia's defensive and offensive cyber capabilities enable us to deter and respond to the threat of cyber attack"[28]. USA has unequivocally stated that when warranted, it will respond to hostile acts in cyberspace as it would to any other[29]. India needs to define its cyber deterrence posture effectively and unequivocally. "Surgical Strikes" in cyberspace can be carried out against our adversaries in a selected case, where attribution is unambiguous. This calls for developing resilience as well as cyber defence and attack capabilities.

[24] Luiijf, E., Besseling, K., & Graff, P.D., "Nineteen National Cyber Security Strategies", International Journal of Critical Infrastructure, 9(1), 3-31, DOI: 10.1504/IJCIS.2013.051608.

[25] NCIIPC, "Guidelines for the Protection of National Critical Information Infrastructure", available at http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf (accessed on 15 June 2017).

[26] Chander, Muktesh, "Protection of National Critical Information Infrastructure", Defence and Security Alert, Vol. 5 Issue 1, pp 54-58.

[27] Wei, Lee Hsiang, "The Challenges of Cyber Deterrence", Pointer: Singapore Journal of Armed Forces, Vol. 41 No1, pp. 12-22.

[28] "Australia's Cyber Security Strategy", available at https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (accessed on 6th June 2017).

[29] White House, "Inter National Strategy for Cyberspace", available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed on 10 June 2017).

10. Cyber Resilience

Absolute security is a myth. In spite of all efforts to secure our digital assets, we must be prepared for cyber attacks. Prediction, prevention, early warning, detection, mitigation, quick & coordinated response and early recovery are parts of cyber resilience plan. If the risk elimination is impossible we must plan to reduce its impact through risk management approach. Adoption of international information security standards, such as ISO 27001 series including ISO22301:2012 for 'Business Continuity Management Systems (BCSMS) – Requirements', must be encouraged in all vulnerable organizations. Adherence to industry specific standards, such as PCI DSS, DSCI Security Framework, COBIT 5, ISACA etc., through a mandatory compliance regime, is the need of the hour. As suggested by Von Solms, we should now adopt Information Security Governance approach driven by the top management[30].

11. Role of Law Enforcement Agencies

Any cyber security breach incident, which is a cognisable crime under Information Technology Act, has to be investigated by law enforcement agencies. Investigation of cyber crimes pose unique challenges due to their peculiar nature. Jurisdictional issues, difficulty in identification & arrest of accused, amorphous nature of evidence, difficulty in identification, collection, preservation and analysis of digital evidence, etc. are some of these issues. The capabilities, infrastructure, tools and other resources, to deal with digital crimes, are far from satisfactory in India. Upgradation of skills of entire criminal justice system, to effectively deal with this challenge, is of vital importance. Cyber forensic labs need more resources to deliver examination results in time. National Cyber Crime Coordination Centre needs to be made operational. Regional and international cooperation to fight cyber crime needs to be strengthened.

12. National Culture of Cyber Security

Most of the recent research has shown that technological measures for cyber security are not enough and there is also a need to understand the impact of human and organizational factors[31]. Al-Wahaibi *et al*. has shown that human factors have a significant impact on the success or failure of information security solutions. Social engineering attacks, particularly those using spear-phishing, exploit human weaknesses[32]. This calls for a nationwide cyber security education and awareness campaign in all organizations. Creation of a culture of cyber security and privacy, enabling responsible user behaviour and actions, through an effective communication and promotion strategy, is one of the objectives of our National Cyber Security Policy. However in a country, where general culture of road safety and sanitation state has much to be achieved, expecting cyber hygiene from every computer user is an uphill task.

13. International Cooperation for Global Cyber Safety

Cyber threats are a global issue. The lack of an international agreement on cybercrime and

[30] Von Solms, B., "Information Security-The Forth Wave", Computers & Security, Vol. 25 Issue 3, pp. 165-168.

[31] Beznosov, K. and Beznosova, O., "On the Imbalance of the Security Problem Space and its Expected Consequences", Information Management & Computer Security, Vol. 15 No. 5, pp. 420-431; Botta, D., Werlinger, R., Gagne´, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B., "Towards Understanding IT Security Professionals and their Tools", in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), ACM, Pittsburgh, PA, July 18-20, 2007, pp. 100-111.

[32] Al-Wahaibi, Said K., Ithnin, N.B. and Al-Badi, A.H., "Information Security Solutions Status and the Roadmap for Future Requirements", Journal of Information Assurance & Cyber Security, Vol. 2011, available at: http://www.ibimapublishing.com/journals/JIACS/2011/664951/664951.pdf (accessed on 13 June2017).

terrorism is thwarting efforts to bring terrorists to justice[33]. International cooperation to fight cyber crime and strengthen global cyber security is essential. With this aim in mind International Telecommunication Union (ITU) has launched Global Cyber Security Agenda as a framework for international cooperation, aimed at enhancing confidence and security in the information society[34]. United Nation General Assembly has passed several resolutions highlighting the role of international cooperation in establishing a global cyber security environment. In year 2001, UN General Assembly Resolutions 55/63 and 56/121 advocated a global framework to counter cyber crime. During its 58th session in year 2003, the United Nations General Assembly passed Resolution 58/199, which sought to outline a basic framework for the creation of a global cyber security regime through the protection of critical infrastructure. International Multilateral Partnership Against Cyber Threats (IMPACT), with a membership of about 145 countries, is also working in the field of enhancing capabilities to address cyber threats with partnership from industry, academia and other international organizations. These global as well as regional efforts need to be continued towards achieving the goal of a UN treaty on Cyber Security.

14. Conclusion and Recommendations

India has taken several measures to deal with the challenges posed by cyber crimes and cyber attacks on CII. However, the response needs to be dynamic and upgraded according to the constantly changing cyber threat landscape. We need to enact a comprehensive Cyber Security Act. There is a need to augment the cyber investigation and cyber forensics labs to deal with growing number of cyber crimes and security breach incidents. Monitoring of social media contents for actionable intelligence needs special attention. Academia, industry and government must come together for developing indigenous cyber security technologies. At present, there are several agencies handling various tasks related to cyber security and there is a need for an apex body to coordinate and synergise the efforts of these agencies. NCIIPC Guidelines need to be made mandatory for critical sectors and sector specific guidelines must be framed. Sensitive organizations must have a Chief Information Security Officer with adequate resources. A 'state of the art' National Cyber Security Operation Centre needs to be established for monitoring cyber attacks on our critical networks and protected systems on 24X7 basis. After the announcement of National Cyber Security Policy, serious steps are required to be taken towards its effective implementation. A continuous education and an awareness drive for all stake holders are required. We need not wait for a 26/11 type attack on our cyberspace to proceed proactively in the direction of developing defensive and offensive capabilities to deal with emerging cyber threats. While walking the path towards a Digital India, we must also transform India from IT power to cyber power[35]. In order to realise the vision of building a secure and resilient cyberspace for our netizens, businesses and Government, holistic cyber security will have to be given due importance in the overall National Security Strategy of India.

---

[33] UNODC, "The use of the Internet for terrorist purposes', available at http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed on 9th June 2017).

[34] GCA, "ITU Global Cybersecurity Agenda", available at http://www.ifap.ru/library/book169.pdf (accessed on 8th June 2017).

[35] Chander , Muktesh, "Cyber Security of Digital India", Defence and Security Alert, September 2015, pp. 54-55.