ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 14, Issue 11,Nov 2024 Impact Factor 8.049 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

CYBER WARFARE IN A MODERN CONTEXT

Dr. Ajay Kumar Pandey, Associate Profesher
Defence and Strategic Studies
S.M.M.Town P.G. College, Ballia (U.P.)

The cyber security threats emanating from malware like stuxnet,Duqu,Flame, Uroburos/ Snake, Blackshades, FinFisher, Gameover Zeus (GOZ), etc are now well known. No country can afford to ignore these cyber threats as computer systems are now essential part of day to day functioning of governments around the world. The cyberspace landscape of India is also fast changing and suitable policies must be formulated by the Modi government to tackle the same effectively. Cyber security is an international issue and it requires international cooperation to be effective. For instance, the cyber security threats emanating from malware like Stuxnet, Duqu,

breach of EBay has international legal ramifications and one can not contend that the place of establishment alone would feel the consequences. However, there are some nations that are not in favors of international technology transfer in the field of cyber security. In one such incidence, India has opposed the proposal to include cyber security technologies under the Wassenaar Arrangement .However, cyber security in India is in a poor condition. Cyber security of banks in India is also required to be strengthened. The banks operating in India are not at all serious about maintaining cyber security of banking related transactions and this is resulting in many cyber and financial crimes in India. In the absence of appropriate skills development and modernization of law enforcement agencies of India, police force are finding it really difficult to solve technology related crimes. Further, cyber security of sensitive databases like National Identity Cards would also require strong privacy protection and cyber security compliances. Another problematic are is absence of an implementable telecom security policy of India. Most of the policies and regulations in this regard are clearly unconstitutional neither in nature as they are neither balanced nor in compliance with the constitutional requirements. Experts believe that the stand of Modi government regarding surveillance projects like Central Monitoring System (CMS) Project of India and Internet Spy System Network and Traffic Analysis System (NETRA) of India must be made clear. Otherwise, this would create troubles for the government as well as for the telecom security policy in the near future.

The cyber security challenges for the Modi government must be given due importance. Cyber security should be an essential component of the national security policy of India. The cyber security trends in India 2013 have highlighted major shortcomings of Indian cyber security initiatives and the same must be addressed by Modi government as soon as possible. Although National Cyber Security Policy (NSCP) 2013 has been declared yet it needs both updation and implementation as per opinion of cyber security experts. We need dedicated cyber security laws in India and effective cyber security policies. For instance, we have no cyber warfare policy of India and this is a major lacuna in the contemporary times. Similarly, critical infrastructure protection in India is also not up to the mark and it needs to be strengthened.[1]

National Cyber Security Policy of India 2013

The National Cyber Security Policy of India 2013 (NCSP 2013) was recently declared by Indian Government. It is a Good Policy on many counts but it also failed to address many crucial aspects as well. For instance, the National Cyber Security Policy of India has failed to protect Privacy Rights in India. Nevertheless, this is a good step in the right direction and it must be updated and improved as the time passes.6 A Cyber Security Policy must be Techno Legal and Holistic in nature. It must be Techno Legal in nature so that it can accommodate both Technological and Legal aspects. It must be Holistic as it should cover as much areas as possible. It must be realistic as well as a single Policy cannot be considered to be Panacea for all Cyber Crimes and Cyber Attacks against India. Thus, the Indian Cyber Security Policy must be supplemented by other Techno Legal Policies. For instance, the E-Mail Policy of India must supplement the Cyber Security Policy. The Cyber Security Policy must also be supplemented with the Telecom Security Policy of India and National Telecom Policy of India 2012 (NTP 2012). In fact, the National Security Policy of India must have the Cyber Security Policy as an essential component. This NCSP 2013 intends to protect information and information infrastructure in Cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and National Cyber Security Policy Of India 2013 (NCSP 2013). The NCSP 2013 aims at facilitating creation of Secure Computing Environment and enabling adequate trust and condense in electronic transactions and also guiding stakeholders' actions for protection of Cyberspace. It outlines a road-map to create a framework for comprehensive, collaborative and collective response to deal with the issue of Cyber Security at all levels within the country. It also recognises the need for objectives and strategies that need to be adopted both at the National level as well as International level.14

The NCSP 2013 envisages a vision and mission statement aimed at building a secure and resilience Cyberspace for citizens, businesses and Government. It strives to enable goals aimed at reducing national vulnerability to cyber attacks, preventing cyber attacks and cyber crimes, minimising response and recover time and effective cyber crime investigation and prosecution. It intends to facilitate monitoring key trends at the national level such as trends in cyber security compliance, cyber attacks, and cyber crime and cyber infrastructure growth.

The Objectives of the NCSP 2013 include to create a secure cyber ecosystem in the country, generate adequate trust and condense in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy, to create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology and people), to strengthen the Regulatory Framework for ensuring a Secure Cyberspace Ecosystem, to enhance and create National and Sect oral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions, to improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product, to create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training, to provide scale beneath to businesses for adoption of standard security practices and processes, to enable Protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft, to enable effective prevention, investigation and prosecution of cyber crime and enhancement of low enforcement capabilities through appropriate Legislative Intervention.[2]

The federal government of the United States admits that the electric power grid is susceptible to cyber warfare. The United States Department of Homeland Security works with industry to identify vulnerabilities and to help industry enhance the security of control system networks, the federal governments also working to ensure that security is built in as the next generation of "smart grid" networks is developed.[3] In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack.Chinadenies intruding into the U.S. electrical grid. One countermeasure would be to disconnect the power grid from the Internet and run the net with droop speed control only. Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma. Howard

Schmidt, former Cyber Security Coordinator of the US, commented on those possibilities. It's possible that hackers have gotten into administrative computer systems of utility companies, but says those aren't linked to the equipment controlling the grid, at least not in developed countries.[4]

The purpose of cyber warfare is to undertake defensive and offensive information operation in the cyber space to degrade the adversary's sensory, early warning, data analysis, intelligence exchange, decision.

support, and command, control and communication network. The entire system of military net-centricity in short while at the same time protecting own information assets from hostile intrusion. In offensive operation, that goal is achieved by intrusion into the adversary' vast volume of digitized information that circulates in cyber space. Notably however in defensive mode, besides adaptation of general security measure, the effort cannot be so much in locking up own volume of information simply because in the cyber domain that is impractical to achieve. The effort therefore is to identify the algorithms and process of the adversary' offensive information operation and neutralize these through corresponding counter offensive measure preferably proactive. Objective of cyber warfare therefore is to gain information superiority in the aspect of surveillance and reconnaissance, data analysis, intelligence exchange, command control of battle element and flow of communication, and thereby protect own net-centric system while disrupting that of the adversary.[5]

Cyber warfare against India has always been confused with minor cyber breaches like websites defacements and cracking into email accounts. India has also been very late in recognizing the need for a robust cyber security. Even the national cyber security policy of India 2013 (NCSP 2013) was declared belatedly and it is still waiting for its implementation.[6] India has no cyber warfare policy till date.

International legal issues of cyber attacks, cyber terrorism, cyber espionage, cyber warfare and cyber crimes in general and international legal issues of cyber attacks and Indian perspective in particular must be understood thoroughly by Indian government to fight against cyber warfare.

The Department of Information Technology created the Indian Computer Emergency Response Team in 2004 to thwart cyber attacks in India. That year; there were 23 reported cyber security

breaches. In 2011, there were 13,301. That year, the government created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defence, space and other sensitive areas. However, there is no public face of NCIPC and some experts believe that NCIPC has failed to materialize and perform its job. It was also reported that National Technical Research Organization (NTRO) would protect the critical ICT infrastructures of India. However, critical infrastructure protection in India has its own challenges that Indian government has not appreciated till now. The Executive Director of the Nuclear Power Corporation of India (NPCIL) stated in February 2013 that his company alone was forced to block up to ten targeted attacks a day. CERT In was left to protect less critical sectors. A high profile cyber attack on 12 July 2012 breached the email accounts of about 12,000people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organization, and the IndoTibetan Border Police (ITBP).[7] A government private sector plan being overseen by National Security Advisor (NSA) Shivshankar Menon began in October2012, and intends to beef up India's cyber security capabilities in the light of a group of experts findings that India faces a 470,000 shortfall of such experts despite the country's reputation of being an IT and software powerhouse.[8]

Conclusion

Being a relatively new form, it is important to develop indigenous postulations concept and practices of cyber warfare in the Indian context. We suggest that the term cyber warfare be usable in the context of military operation, as distinct from the overarching scheme of cyber warfare at the national level. It also posit that when prosecuted under the overall ambit of information operation, cyber warfare is predominant in offensive content and may be conduct from space, earth and cyber space. Further, it implies that: firstly, continuous engagement in information operation during peace keeps the system fully updated and promotes experimentation and sprit of innovations; and secondly, readiness for instant engagement is an imperative of cyber warfare. It is also reiterated that most of the principle and activities associated with cyber ware fare are applicable, with certain reorientations, to the civil

information infrastructure too.

References

1. Cyber security in india.http://cybersecurityforindia.blogspot.in/ 12/14. 11/08/2015.

2. Analysis of national cyber security policy of India (NCSP-2013)And Indian cyber security infrastructure, Nov21,2014.

3. "Cyber attacks, Terrorism Top U.S. Security Threat Report" (http://www.npr.org/2013/03/12/174135800/ cyberattacksterrorismtopussecuritythreatreport).NPR.org.12March 2013

4."Clarke: More defense needed in cyberspace" (http://www.hometownannapolis.com/news/top/2010/09/2411/ ClarkeMoredefenseneededincyberspace.html) HometownAnnapolis.com, 24 September 2010**.**

5. Lt.Gen Gautama Banerjee, visiting fellow, VIF "cyber warfare in Indian context".

6. "National Cyber Security Policy of India 2013 (NCSP 2013)" (http://perry4law.org/cecsrdi/?p=1068). Centre of Excellence For Cyber Security Research And Development in India. Retrieved 14 August 2014.

7. "Beware of the bugs: Can cyber attacks on India's critical infrastructure be thwarted?" (http://businesstoday.intoday.in/story/ indiacybersecurityatrisk/1/191786.html). Business Today. Retrieved January 2013.

8. "5 lakh cyber warriors to bolster India's e-defence" (http://articles.timesofindia.indiatimes.com/20121016/india/ 34498075_1_cybersecuritycyberattackscyberwarfare). The Times of India (India). 16 October 2012. Retrieved 18 October 2012.

9. Self Theam