Cyber Security in India: Problems and Prospects

Sushma Devi*
Mohd. Aarif Rather**

Abstract

Cyber security has emerged in the backdrop of information, communication and technological revolution and acts as the corner stone of a connected world. Within the purview of this revolution, the international community across the globe came in confrontation with the new domain of cyber world where opportunities, e.g. communication as well as challenges are becoming paramount. Thus, the world is witnessing different hazards and dangers which have never been experienced in previous periods of history and India is no exception to this. Also, in contemporary times, the current threats faced by the global security environment emerge from the technological progress and were not bound by local origins but extends to include the global networks. Such threats transcend the limits of time and space boundaries and present a continuous and universal challenge. Thus, the inter-state relations drown into securing their economic and security threats without imposing severe restriction on cyber world. In addition, cyber-attacks have the potential to push the states into real acts of aggression and there exists no balance of power in the cyber world. In this context, the paper tries to explore the areas of cyber security out of conventional notions of security and situate India at threshold of analysis with taking different countries responses into consideration. Also, an attempt is made to identify challenges as well as possible diagnosis.

Keywords: Cyber security, India, information, technology, threats, global security.

Introduction

The concept of security existed from times immemorial, but has assumed wider dimensions in contemporary times. In common usage, it is connected with a series of different aspects of human existence and with the processes and activities in society and nature. In International relations, the concept came into existence after the end of 2nd World War. But, it was largely assumed to be based on the realistic paradigm i.e., global politics is always a struggle between nations to reach power under a condition of anarchy in which they compete for their respective national interests. Thus, the security was related to the protection of states alone in terms of political stability, territorial integrity and sovereignty. However, after the end of the cold war, the concept of the security underwent a change from state-centric notion to individual centred.As such, the individuals became the referent objects of security. The nature of threats changed from external aggression to intra-state conflicts[27]. Such threats range from civil wars to environmental degradation, from economic deprivation to human right violation and so on. Apart from these threats, the global politics witnesses the age of information, communication and technology which revolutionised every aspect of human life. It is within the back-drop of this technological revolution that the concept of cyber security came into existence and assumed top priority at global level.

The Network outages, computer viruses, data conceded by hackers and other incidents in one way or the other affect our lives that range from troublesome to life-threatening. The term "Cyber security" refers to securing information technology and focussing on protecting computers, programs, networks and data from unauthorized or unintended access from change or destruction. As most of the government and financial institutions, military groups, corporations, hospitals and other businesses

Sushma Devi*
Research Scholar,
Centre for Security Studies, School of International Studies, Central University of Gujarat

Mohd. Aarif Rather**
Research Scholar,
Centre for Security Studies, School of International Studies, Central University of Gujarat

entrepreneurs store and process an abundant deal of confidential information on computers. Such important data is transmitted across networks to other computers. However, with the increasing volume and sophistication of cyber-attacks, the on-going attention is needed to protect personal information and sensitive business as well as to safeguard the national security. On the other hand, Cyber security plays a vital role in the current development of information technology and Internet services [41]. Therefore, it becomes essential for each nation's security and economic well-being to enhance the cyber security and protecting critical information infrastructures. To make the Internet safer has become integral to the development of government policy as well as new services[9].

The concern of cyber security although in the emerging phase has appeared as an important ingredient in the conduct of international relations in contemporary times. It has already started influencing the relations between states. For instance, in recent years, the concern over cyber security has become a contentious issue between U.S - China relations. The U.S has been alleged China of digital espionage against its business and strategic interests as well as targeting proprietary economic data and sensitive national security information. On the other hand, China also claims U.S of being accused of website defacements, network exploitation and service denials attacks. This kind of situation exacerbates mistrust and raises suspicions in both the states regarding the others activities and motives [5].

The cyber-space is evolving as a place where the states are imitating their actions in the real world diplomacy as well as their relations between or among them. It has steadily becoming an arena where states need to protect their territory. Thus, there existed a vital need to apply tools and methods to extract the maximum out of the cyber world in order to serve their national as well as collective interests.Many countries has witnessed several cyber security threats mainly from 2010 onwards and India is no exception to it. For instance, in 2012, some suspected Iranian hackers hacked around 30,000 computers of the Saudi Arabian Oil Company namely "Saudi Aramco" and rendering them useless. The aim of this cyber-attack was to stop the flow of Saudi oil. Similar kind of attack was also launched against the world's largest liquefied natural gas suppliers "RasGas" a joint-stock company owned by Qatar Petroleum and ExxonMobil which also suffered from the similar damage[7]. In addition, in March 2013, North Korea launched a digital destruction against South Korea by attacking its three TV stations and three banks. Thus, the present decade witnessed numerous cyber security attacks mainly aimed to destruct economic set-up as well as the state's national security.

In the Indian context, the issue of cyber security has received less attention from the policy makers from time to time. The governments have been unable to tackle the growing needs for effective and strong cyber security of India. The reason behind is that India lacks the offensive and defensive cyber security capabilities necessary to tackle the cyber security attacks. Also, India is not boosted with such mechanisms that are vital to confront with sophisticated malware like Stuxnet, Flame, Black shades etc. Thus, the cyber security trends in India seems to be unconvincing at all [19].

Historical Background of Cyber Security

The history of cyber security can be traced back to 1970's when the first computer hackers appeared as they tried to circumvent the system and attempted to make free phone calls. However, it was only after the mid 1980's that the first computer virus called "Brain" was created and as such the Computer Fraud and Abuse Act were established in 1986. Also, in 1990's, several notable threats came into existence affecting the modern information security industry. The Distributed denial of service attacks as well as the bots that made them possible also came into being. Moreover, in early decade of 21st century, this malicious Internet activity assumed the shape of a major criminal enterprise aimed at monetary gain [30]. Such activities entered into mainstream by primarily targeting online banking and then moving onto social networking sites [25]. Now a day, the cyber issues has assumed a much larger dimension and had a greater impact on the national security of states.

With the advent of globalisation process, the world has become more interconnected and the number of Internet hosts and the personal computer industry has

increased. As a result, the large number of people got access to Internet. The everyday life witnessed more people coming online, more things connected to internet, the public sector increasingly leveraging ICTs vis-à-vis the consequences of cyber-attack raised. Under such an open and wide platform, the Internet remained no longer safe [1].The issues of privacy and security concerns emerged and as such the concept of cyber security came more into picture. Presently, cyber security has become a global concern and includes within its ambit the issues like Cyber warfare, Cyber-crime and Cyber terrorism.

Cyber warfare, Cyber terrorism and Cyber-crime

In contemporary times, computers play an important role in the battlefields in controlling targeting systems, managing logistics as well as in relaying critical intelligence information. Also, at both the strategic as well as tactical levels, the battlefields stand to be fundamentally altered by the information technologies. Therefore, the increasing depth and breadth of this battlefield as well as the improving accuracy and destructiveness of even conventional weaponries have heightened the importance of Control, Command, Communications and Intelligence matters. The dominance in this particular aspect may now yield the advantages of consistent war-winning [2].

Cyber warfare

Cyber warfare is comparatively a new type of weaponry having various effects on the target. It is beyond any limitations of use and can be useful in achieving most of the set goals. The history revealed that military organizations, doctrines and strategies have frequently undergone profound changes due to the technological breakthroughs. Also, the information revolution crosses across borders and thus it generally compels closed systems to open up. This led a direct impact on the future of the military as well as of conflict and warfare more commonly. Thus, cyber warfare revolves around information and communications matters at much deeper levels. The cyber war may be applicable in conventional and non-conventional environments, low as well as high-intensity conflicts and for offensive or defensive purposes. In broader sense, cyber war indicates a transformation in the nature of war [2].

Cyber Warfare has become a more powerful instrument in today's battlefield and had large impact on the development of armies as well as weapon technologies in many countries. In mid-2007, the Israeli cyber warriors hacked the Syrian anti-aircraft installations and reprogrammed their computers. The installation system of Syrian's computers displayed an empty sky. By doing so, the Syrian's allowed Israeli planes to bomb over a suspected nuclear weapons manufacturing industry. The first among known cyber-attacks was launched by the Russia under Deliberate Denial of Service (DDOS) against "Paperless government" of Estonia. After this attack, the DDOS emerged as a common platform of attack for countries like U.S., China, Russia, North Korea, Israel and Pakistan [31]. The analysts around the globe are conscious about the fact that any large-scaled future conflict will comprise cyber warfare as part of a combined arms effort [6].

Cybercrime

Cybercrime refers to any illegal activity by using computers as a primary mode of commission. Cybercriminals use computer technology to access business trade secrets, personal information or using the Internet for malicious or exploitive purposes. The information stolen by the criminal's affects hundreds of millions of people in their day today affairs. It has been estimated that in 2012, 54 million people in Turkey, 40 million in the US, 20 million in Korea, 20 million in China and more than 16 million in Germany have been affected by the cybercrimes. The growth is still alarming and is expected to be more than 800 million in 2013 at global level. The cybercrime is thus a biggest problem affecting both the developed as well as developing world. The consequences of cybercrime had bad implications on the trade, innovation, competitiveness and global economic growth [16]. However, the problem associated with the Cybercrime is that the perpetrators no longer require complex techniques or skills.

On the other hand, the intensity and perceptions of relative risk and threat largely vary between Governments and private sector enterprises. From the perspectives of national security, almost two-thirds of countries view their systems of police statistics insufficient for recording cybercrime. According to the

Police-recorded cybercrime rates, the number of crimes is associated with levels of country's development vis-a-vis specialized police capacity rather than underlying crime rates [36].

In 2000, the first major instance of cybercrime took place when a mass-mailed computer virus affected around 45 million computer users worldwide. However, the cybercrime landscape changed dramatically and began to attain the politically motivated objectives. In the last decade, cyber-attacks have been evolved in utilizing the online weapons affecting several government entities. The cyber experts are of the view that the world has witnessed glimpses of cyber war with unethical cyber hackers stealing important state information. Quoting US Defense Secretary Robert Gates, "cyberspace is the new domain in which war will be fought after land, sea, air and space" [20].

The present age i.e., digital age has witnessed a norm of online communication in which the internet users as well as governments confront with becoming the targets of cyber-attack. With the advancement in the techniques of cyber criminals, their focus shifted from financial information to business espionage as well as accessing government information. To fight fast-spreading cybercrime, governments must collaborate globally to develop an effective model that will control the threat internet-based networking, cybercrime and digital attack incidents have increased around the world [20].

Cyber terrorism

Cyber terrorism is any deliberate attack against information of computer systems, programs and data resulting in violence against non-combatant targets by secret agents or sub-national groups. The attacks are generally politically motivated. The cyber-attacks are designed to cause extreme financial harm or physical violence. The thrust areas of cyber terrorist targets include military installations, banking industry, air traffic control centres, power plants and water systems etc. The term 'Cyber terrorism' is sometimes referred to as information war or electronic terrorism [28].

The present global era has witnessed more than one billion online users and 233 countries connected to the Internet. In such an inter-connected world, terrorism is flourishing through terrorist's use of information and communication technologies (ICTs). Today, nearly all the terrorist organizations either small or large have their own Web sites. The recent example of terrorist attacks includes Osama Bin Laden, attack on America's army deployment system during Iraq war and the LTTE. The terrorist organisations cooperate with organized crime vis-a-vis use technology to spread propaganda, recruit and train members, raise funds, communicate and launch attacks. The reason in making the internet as an attractive medium is the technological difficulty in dealing with cyber communications. Also, the governments face several difficulties in combating with terrorist's use of ICTs which include the lack of coordinated procedures and laws in investigating cybercrimes, ineffective or inadequate information sharing and complications in tracing and tracking cyber communications [41]. Therefore, a global attention is needed to address these areas of cyber security in order to win the battle against terror.

Cyber Security and International Community

In recent decades, cyber security has emerged as a global phenomenon and the most critical concerns of the IT age. It acts as the corner stone of a connected world. To address this issue, a truly global approach is needed. Because of its universal networks, cyber terrorists and criminals do not need their presence anywhere near the scene of the crime [1]. Therefore, international response and cooperation is needed to address the notion of cyber security properly.

Cyber Security under United Nations

United Nations since its inception has taken the responsibility of maintaining peace, security and cooperation among the member-states. So far as the issue of cyber security is concerned, it had established Information Telecommunication Union (ITU) in 1965 to ensure the safety of all those who venture online. ITU is the leading agency of United Nations for information and communication technologies and a global focal point for the private sectors as well as governments. The purpose of ITU is to focus on the growth and development of information and telecommunication networks as well as to enable global

access to all the people so that they may easily participate and avail the benefits from the global economy and emerging information society [17].

Apart from ITU, the United Nations has expressed itself on cyber security matters and passed five major Resolutions in this regard. The first resolution under A/RES/55/63 was issued on December, 4th 2000 dealing with the criminal misuse of ICT's. It identifies that the unrestricted flow of information can promote social and economic development as well as can be useful in sustaining democratic governance. Another resolution issued on 19th Dec, 2001 by the UN under A/RES/56/121 requested the states to cooperate and coordinate against misuse of ICTs. Basically, the primary purpose of the resolution was to set the national laws and policies to address the crimes related to computer.

On 20th Dec, 2002, the UN passed a resolution under A/RES/57/239 emphasising on the establishment of global culture of cyber security. It urged the need that the law enforcement as well as separate governments cannot address cyber security alone but demands global attention and cooperation. The UNs fourth resolution (A/RES/58/199) issued on 23rd December 2003 also deals on the global culture of cyber security but at the same time focused on the protection of critical information infrastructures like maritime and air transport, financial and banking services, food distribution, water supply and public health [40].

In 2010, the UN appointed three Groups of Governmental Experts (GGE) to examine the prevailing and potential threats from the cyber-sphere as well as to find measures so as to combat them. Also, in 2011, a resolution under A/RES/66/24 was passed by the General Assembly emphasis the need of addressing the assessments and recommendations as contained in the Report of 2010 [35]. In addition, the UN Secretary-General Ban Ki-moon appointed the group of 15 experts on 9th August 2012 to draft a report on the Developments in the Field of Information and Telecommunications from the perspective of International Security. The experts include the five permanent members of the UN Security Council as well as India, Japan, Canada, Belarus, Australia, Egypt, Germany, Argentina, Estonia and Indonesia. The experts emphasis that there is a need to elaborate confidence-building measures and to set several rules and principles of responsible behaviour of States with respect to cyber security [42].

Again in 2013, the UN General Assembly adopted a resolution under 68/243 in which special attention was to be laid on the outcome of the 2012/2013 GGE. Also, the Secretary-General of UN was requested to establish a new GGE that would report to the General Assembly in 2015 [35].To sum up, it may be assessed that the issues of cyber security are quickly making its way into the agenda of global public policy issues and thereby demanding proper attention [23].

Canada's Cyber Security policy

The cyber security strategy was issued by the government of Canada in October 2010. The basic purpose of the strategy was to secure the government systems, to protect vital cyber systems outside the federal government so as to strengthen resiliency and facilitating Canadians to be secure online [37]. The Security Intelligence Service of Canada considers the cyber threat as one of its five priority areas including security screening, proliferation of weapons of mass destruction, terrorism and finally espionage and foreign interference[37]. The strategy also focused on the need to have an international engagement between the allied militaries and Department of National Defence on cyber defence for an effective implementation of such practices [12]. The responsibility of handling the computer and communications networks of the armed forces have been entrusted with the Canadian Armed Forces Information Management Group. In addition, the government of Canada established the Directorate of Cybernetics in June 2011 to enhance the cyber warfare capabilities for the armed forces [37]. Thus, the Canada has taken some positive steps in the direction of improving the cyber security dimensions.

China's Cyber Security policy

In early 2011, the government of China's Information Office issued a white paper on national defence by which it directed the military to maintain its security interests in cyber and electromagnetic space. It focuses that the fighting capabilities of the armed forces in circumstances of informationization have been

considerably raised. As such, there is a need to raise a new type of combatting capability so as to win local wars in conditions of informationization [15]. In the same year in May 2011, the Chinese Ministry of National Defence declared that the army had set up an "Online Blue Army" in order to improve the cyber security of the military forces [43].

In 2012, the Republic of China issued a set of new policy guidelines for cyber security. It urged the need for bringing the efforts to better handle and detect information emergencies, protect personal information and to reduce internet crime [44]. The Ministry of Public Security and the Ministry of Industry and Information Technology in China have taken the responsibility for securing the cyber security sector. Apart from the improvements made by china in the sector of cyber security, the country had witnessed several emerging threats in this particular sector. But at the same time, it has evolved as one of the major cyber security nations in the world.

United States (US) Cyber Security policy

In 2009, the United States formulated a Cyberspace Policy Review and also appointed a mid-level Cyber security Coordinator to the members of the National Security Council [37]. In 2010, it retained some of the provisions of Cyberspace Policy Review in its National Security Strategy [38]. The responsibility of dealing with the cyber security issues is entrusted with the Department of Homeland Security, the Department of Defence and the Bureau of Investigation. However, the major step taken by US in the direction of cyber security was initiated in 2012 under an extensive cyber security programme in the realm of both civilian as well as military aspects. In the same year, in October, President Obama signed a Presidential Decision Directive regarding the activities in cyberspace. The directive makes it clear that the military will have a greater role to play in defending against cyber-attack from foreign invasions[23]. Also, in November, the Defense Advanced Research Projects Agency of UN released a document called Foundational Cyber warfare asking for research into the conduct of cyber war. The document stated that there is a need to investigate into the nature of cyber warfare and to find out the strategies needed to dominate the cyber battle space [37]. Thus, the US has taken some vital steps towards strengthening its cyber security agenda. The progress made by the US in the cyber security sector becomes clear by the cyber-attack "Stuxnet" against an Iranian nuclear facility in 2010 [29].

United Kingdom's (UK) Cyber Security policy

In contemporary times, the UK has one of the most advanced national cyber security approaches. In the year 2011, the UK restructured its Cyber Security Strategy in which cyber- attack was considered as a national security threat. The basic objectives of the strategy include addressing cybercrime, enhancing information infrastructure resiliency, ensuring a safe cyberspace for the public and evolving an adequate cyber security workforce. Apart from this, the strategy makes it clear that the UK will work bilaterally as well as through international forums to establish international norms in the realm of cyber security and will also work to develop confidence-building measures in this sector [34]. The UK government has allocated £650 million through 2015 for implementing the National Cyber Security Programme [12].

In 2012, the UK announced the establishment of an academic institute for the purpose of researching cyber security. The objective behind was to increase resiliency against the cyber- attack as well as to better equip the government to defend the country's national interests in cyberspace [21]. Also, the UK government intends to establish a National Crime Agency to investigate and respond to serious national-level cybercrime as well as provide training and support to local police forces to deal with such crimes [34]. In addition, the Defence Cyber Operations Group will be created which would be operational by March 2015. The Group would consist a federation of cyber units across defence to safeguard the comprehensible integration of cyber activities across the spectrum of defence operations [33].

Russian Federation's Cyber Security policy

The national policy for fighting cybercrime and the establishment of a national system to prevent and detect cyber-attack was released by the Russian Federation's Security Council in July 2012. The

Responsibility for implementing the policy was given to the Federal Security Service. The aim of the policy is to secure the country's networks from foreign sources [4]. Also, the government has drafted a bill to make an advanced military research agency for dealing with cyber security. The bill discusses the principles of information security and different measures to control for interference in information systems. Thus, the Russian federation seems to be determinant to protect national interest's vis-à-vis recognising the greater role of information warfare [37].

To sum up, it may be assumed that various nations particularly the developed ones have taken some serious steps in combatting with the cyber security issues. At the same time, they have initiated various policies and programme to enhance and strengthen their cyber security sectors.

Indian perspectives of cyber security

The IT sector in India has emerged as one of the most significant growth catalysts for its economy. Also, this sector is positively influencing the lives of its people either through direct or indirect contribution to several socio-economic parameters like standard of living, employment, diversity among others etc. In addition, it has played a vital role in transforming India as a global player. Further, the Government sector has facilitated increased adoption of IT sectors in the country that encourage IT acceptance and National programmes like Unique Identification Development Authority of India (UIDAI) and National e-governance Programmes (NeGP). The adoption of such programmes has created large scale IT infrastructure and promoted corporate participation. However, despite the growth in IT sectors of India, there has been a tremendous need to secure computing environment as well as build adequate confidence & trust in this sector. The presence of such environment enables a need for the creation of suitable cyber security eco system in the country [13].

The last couple of decades witnessed India in the niche of IT. Almost, all the financial institutions as well as Indian banking industry have incorporated IT to its full optimization. At the same time, these economic and financial institutions are confronted with cyber-attacks in their daily activities. However, the increasing dependency of these Indian institutions on IT under cyber threats might lead them to an irreparable collapse of economic structures. Although, the worrying part is that there is absence of alternatives to tackle with these kinds of threats [26].

In India, several organisations within the ambit of Ministry of Defence have taken the responsibility of dealing with the concept of cyber security. In the year 2005, the Indian Army formed the Cyber Security Establishment in order to protect the networks at the division level as well as to conduct safe cyber security audits [24]. Also, in the year 2010, the army established the Cyber Security Laboratory at the Military College of Telecommunications Engineering in Madhya Pradesh with a view to provide specialized training to its officers in security protocols for its signal as well as data transmission networks [10].

In March 2011, the Indian Ministry of Communications and Information Technology released a draft on National Cyber Security Policy. The policy mainly focused on the security and protection of critical infrastructure, development efforts as well as public–private partnerships [13]. In June 2012, a proposal in line with the draft policy under National Security Council intends to create the National Critical Information Infrastructure Protection Centre (under the National Technical Research Organisation). The objective behind this was to ensure the security of the state's critical infrastructure along with national and sector-specific Computer Emergency Response Teams (CERTs) [18]. In the same year in May, the Indian Ministry of Defence Research and Development Organization have established an indigenous system of cyber defence to ensure that network sectors are safe and secure. The project was reportedly about 50 percent to be complete as of May 2012 [45]. In the context of cyber security, the Technical Intelligence Communication Centre and the National Defence Intelligence Agency are creating a joint team to aware the government about potential cyber vulnerabilities [32].

Apart from taking several positive steps, the cyber security projects and initiatives in India are still very less in numbers as compared to other developed nations. Some of the projects proposed by the Indian

government have even remained on papers only. In addition, the Projects like National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) of India has eventually failed to materialise so far. Also, the National Cyber Security Policy of India framed in 2013 failed to show fruitful results and even its implementations seems to be weak on numerous aspects. On the other hand, there is a vital need to protect the critical infrastructures such as banks, satellites, automated power grids, thermal power plants etc from the cyber-attacks in India [32]. The Indian government claimed that there has been a huge rise in cyber-attacks against the establishments like the banking and financial services sector. In the year 2013,there was a 136% increase in cyber-threats and attacks against government organizations as well as 126% against financial services organizations in India [3]. Also, the country ranks 7th in the cyber-attacks and 85th in the net connectivity [8]. In addition, the India continues to be an attractive target in recent times for cyber criminals with around 69 percent targeted attacks being focussed on large enterprises. According to the report by security software maker 'Symantec' India nearly witnesses four out of ten attacks which are carried on non-traditional service industries like business, hospitality and personal services [14]. Thus, there exists a vital need for India to frame a cyber-crisis management plan in order to combat with the cyber threats effectively.

Refrences

1. Andreasson, K.,Cyber Security: Public Sector Threats and Responses, New York: Auerbach Publications,2012.
2. Arquilla, J. and Ronfeldt, D.,"Cyberwar is coming,"Comparative Strategy,vol. 12, no. 2, pp. 141-165, 1993.
3. Athavale, D.,"Cyberattacks on the rise in India,"The Times of India, 10 March, 2014.
4. C.news., "Russia rolls out state cyber security policy," Russia, 12 July, 2012.
5. IGCC Report,"China and Cybersecurity: China and Cybersecurity: Political, Economic, and Strategic Dimensions,"Report from Workshops held at the University of California, San Diego, April 2012, pp. 1-34.
6. Clarke, R. A., and Knake, R.,Cyber War: The Next Threat to National Security and What to Do About It, USA: Ecco Publications, 2012.
7. Kyrou, D.K.,"Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges,"Connections, vol. XII,no. 3, pp. 109-117, 2013.
8. Express News Service, "India 7th in Cyber Attacks, 85th in Net Connectivity,"The new Indian express, 01 July, 2014.
9. Gercke., Understanding Cybercrime: a Guide for Developing Countries, Geneva: ITU publication,2009.
10. Governance Now,"Army sets up cybersecurity lab",2010, Available: http://www.governancenow.com/news / regularstory/army-sets-cyber-security-lab.
11. Government of Canada, "Canada's Cyber Security Strategy", 2010,Available: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgyeng.pdf.
12. House of Commons Defence Committee, "Defence and Cyber-Security", London: The Stationery Office Limited, 2013.
13. Indian Ministry of Communications and Information Technology,"National Cyber security Policy", draft v1.0, 26 Mar, 2011.
14. Indo-Asian News Service, "Large films hit by 69 percent of targeted cyber-attacks in India: Symantec", 26, April, 2014.

15. Information Office of the State Council of the People's Republic of China, "China's National Defense in 2010", Information Office of the State Council, The People's Republic of China, March 2011.

16. Intel Security (2014), Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies, USA.

17. International Telecommunication Union, "Agencies of the UN: ITU," 2014, Available**:** http://www.un.cv/agency-itu.php**.**

18. Joseph, J., "India to add muscle to its cyber arsenal," TheTimes of India, 11 June, 2012.

19. Kaushik, R.K., "Cyber Security Needs Urgent Attention of Indian Government,"2014, Available:http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention .html.

20. KPMG International,Cybercrime – a growing challenge for governments, Issues Monitor,vol. 8, no. 3, pp. 1-21,2011.

21. Meyer, D., "Spies and professors band together for UK cyber security research institute," ZD Net, 13 September, 2012.

22. Meyer, P,"Cyber Security Takes the Floor at the UN", Canadian International Council," 12 November 2013.

23. Nakashima, E., "Obama signs secret directive to help thwart cyber-attacks", Washington Post, 14 November, 2012.

24. Pandit, R., "Army gearing up for cyber warfare," Times of India, 7 July, 2005.

25. Pillai, P., "History of Internet Security," 2012,Available URL: http://www.buzzle.com/articles/history-of-internet-security.html.

26. Raghav, S.S.,"Cyber Security in India's Counter Terrorism Strategy", 2009, Available: http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf.

27. Rather, M.A. and Jose, K.,"Human Security: Evolution and Conceptualization,"European Academic Research, vol. II, no. 5,pp. 6766-6797, 2014.

28. Rouse, M.,"Cyber terrorism", [Online: web] Accessed on 16 August, 2014, Available: http://searchsecurity.techtarget.com/definition/cyberterrorism.

29. Sanger, D.E., "Obama order sped up wave of cyberattacks against Iran," New York Times, 1 June, 2012.

30. SC Magazine, "A brief history of internet security," 2009, Available: http://www.scmagazine .com/a-brief-history-of-internet-security/article/149611/.

31. Singh, C.M.,Cyber War and Terrorism, Delhi: Prashant Publishing House, 2009.

32. Singh, H. and Philip J.T., "Spy game: India readies cyber army to hack into hostile nations' computer systems," Economic Times, 6 August, 2010.

33. United Kingdom,"Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", London: The Stationery Office Limited. (2010),

34. United Kingdom, "The UK Cyber security Strategy: Protecting and Promoting the UK in a Digital World," Cabinet Office 22, Whitehall London, pp. 1-43, 2011.

35. United Nations, "Developments in the field of information and telecommunications in the context of international security,"United Nations Publication: New York, pp. 1-56, 2011.

36. United Nations, "Comprehensive Study on Cybercrime," United Nations Publication: New York, pp. 1-287, 2013.

37. United Nations Institute for Disarmament Research,"The Cyber Index: International Security Trends and Realities,"United Nations Publication:New York and Geneva, pp. 1-140, 2013.

38. United States,"National Security Strategy,"2010, Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

39. UNODA, "Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations, New York, 2011.

40. Wamala, F.,"The ITU National Cyber security Strategy Guide,"Telecommunication Standardization Sector of ITU (ITU-T), Geneva, Switzerland, 2011.

41. Westby, J.R., "Countering Terrorism with Cyber Security," Jurimetrics, vol. 47, no. 3, pp. 297-313, 2007.

42. Wolter, D**.**, "The UN Takes a Big Step Forward on Cyber security,"Arms Control Association, 13 September, 2013.

43. Xin, Y, "PLA establishes 'Online Blue Army' to protect network security," People's Daily Online, 26 May, 2011.

44. Xinhua, "China calls for tightened information security measures," China Daily, 18 July, 2012.

45. Xinhua, "India developing cyber defense program,"2012, Available: http://english.cri.cn/6966/2012/05/04/2941s697329.htm.