International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 2; March 2018; Page No. 685-688

The symbiotic nuances of cyber and national security

Divya Dwivedi
Senior Research Fellow, Department of Defence & Strategic Studies, University of Allahabad, Allahabad, Uttar Pradesh, India

Abstract
This paper examines the vital element of National security in today's world of globalization and information cyber security. The internet is revolutionizing our society by providing a fast, inexpensive and easy way to connect people and is an important source to drive economic growth. Internet has become increasingly central to our economy and social relations. There is now a close relationship between the physical world and cyber world and they affect each other. The revolution in the information technology, processes and internet connected computers are altering our way of living- how we communicate, perform banking transactions, make purchases and make use of this in diplomacy and wars. While the cyber world provides a number of facilities, it also brings with it a host of problems for security of communications, data and infrastructure.
This paper shows different aspects of cyber security its objective, functions, threats, challenges etc. and finally conclusion. At present time the development of cyber-assets depend upon how strong protection measure we have devised to protect it. It is the stage when cyber security should be placed at the zenith of priority even if it amounts to certain modifications and alterations in India's cyber domain. If the cyber security of the country is to be preserved the most pertinent consideration is that the security measures must be devised keeping in mind the native conditions and shall be developed by the Indian minds. This consideration again remind us the reason behind formal division of roles and responsibilities between the civil and military functions of cyber security

Keywords: cyber warfare, cyber terrorism, cyber espionage, India's national security, cyber-attacks, cyber security, hacking

1. Introduction
The last two decades have witnessed rapid development and transformation in the realm of cyber space. Today the internet has become an easy to use and inexpensive medium for the government, private sector and individuals. Speedy advances in microprocessor communication especially in the mobile, storage and software technologies have greatly changed the face of government and business practices. The World Wide Web and social media today touch every aspect of human lives. The World Wide Web began only in 1991, and today more than 2 billion people (about 40% of world population) are online at any time with about 5 billion internet connected devices. More are set to join in the coming period.
The internet is revolutionizing our economy as well as the society by providing a fast, inexpensive and easy way to connect people and businesses. There is now a symbiotic relationship between the physical world and cyber world and they affect each other. The revolution in the information technology, processes and internet connected computers are altering our way of living- how we communicate, perform banking transactions, make purchases and make use of this in diplomacy and wars. While the cyber world provides a number facilities, it also brings with it a host of problems for security of communications, data and infrastructure.
The cyber space now occupies a key position in national security. In recent years, large scale cyber threats that includes attacks through virus like Stuxnet, the emergence of hacker networks (comprising individuals, criminal gangs and foreign intelligence agencies supported groups), and the militarisation of cyber space are receiving attention of government and private sector to the vulnerabilities of a networked and digital world. In an effort to address vulnerabilities and related issues, stakeholders across the national security system are actively seeking to develop legal and policy solutions to protect the national assets while limiting regulation and intrusion into what is largely a privately owned and operated domain [1].
India's drive towards digital economy coupled with national projects like Digital India, Smart Cities, National Broadband Network and so on are altering the digital landscape rapidly with direct impact on governance, transparency and accountability. While there is a definite requirement of greater penetration of ICT for development and better governance, this rapid change towards a digital environment has brought to fore the challenges of cyber security. A cyber insecure Digital India Initiative can turn from a strategic asset to an unaffordable liability and a direct threat to national security. India, needs safe navigation through cyberspace for its prosperity, national and human security. Hence, ensuring complete cyber security of our assets and National Information Infrastructure is both a national strategic imperative and an urgent national mission.

2. Threat Analysis
Cyber crimes are a real threat today and are increasing very rapidly both in intensity and complexity with the spread of internet and smart phones. About eighty percent of cyber-attacks are related to cybercrimes. More importantly, cyber-crimes have changed the nature of conflict by blurring the line

between state and non-state actors.

From leaking debit card details to influencing the US Presidential Election, cyber-attacks have become a significant part of our political and social discourse. Cyber threat exists 24/7 and manifests along the full spectrum starting from cybercrime to cyber espionage to cyber terrorism and cyber war.

Cybercrimes are likely to increase exponentially with the fielding of virtual currency, Internet of Things, big data, cloud technology, drones, robotics, Blockchain and so on. Capabilities of hijacking a car, taking over the controls of an aircraft, cyber murder and remote injunction of viruses through drones and air crafts have already been demonstrated and in some cases, already inducted.

Dark net and deep web are already being exploited for sale of vulnerabilities, weapons, recruitment of people in terrorist groups, drugs and so on.

Latest entrant to the long list of cyber-crimes is the installation of "Ransom Ware" to cripple a network or facility and demand ransom to restore the same. Recent ransomware attacks using Wanna Cry and Petya viruses have amply confirmed cyber as a "Weapon of Mass Disruption" with more than 300,000 computers affected across different sectors: health, finance, transport, ports and so on in 150 countries! Another major cyber-attack on HBO is still awaiting resolution with hackers demanding 2.5 million in Bit Coins.

One of the biggest cyber-attack in 2016 was the hacking of Indian debit cards wherein as many as 32 lakh debit cards belonging to various Indian banks were compromised resulting in the loss of Rs. 1.3 crore in fraudulent transactions as per National Payments Corporation of India (NPCI).

The Infamous hacker group "Legion Crew" made headlines in the sub-continent after hacking into the Twitter accounts and partial email dumps of prominent public figures such as politician Rahul Gandhi, businessman Vijay Mallya, and NDTV journalists Barkha Dutt and Ravish Kumar [2].

3. National security paradigm in realm of cyber space

However, while India still ranks higher than global peers when it comes to instances of malware and ransomware attacks at 54% as compared to 47% globally, the silver lining has been the increase in spends on network security by small & medium businesses (SMBs), enterprise as also service providers [3].

National cyber strategy for integrated approach India has taken steps in establishing institutions and released the National Cyber Policy in 2013 to deal with cyber security issues. India has established CERT-IN to increase its ability for situational awareness and provide assistance to victims when the attack takes place. The National Cyber Coordinator has been appointed to analyse the cyber threats. India has also created the National Critical Infrastructure Protection Centre under National Technical Research Organisation (NTRO) for the protection of its vital information centres. NTRO has released the guidelines in this context and provides guidance from time to time. DRDO is involved in cyber research projects. In addition armed forces and intelligence agencies have their own units to meet their operational requirements.

Notwithstanding the above, India is facing problems in securing a credible cyber system. The National Cyber Policy is overly prescriptive and is not geared to deal adequately with the fast changing nature of cyber threats. Currently all institutions work in silos. India needs to acknowledge that the vulnerabilities do not merely arise from inadequacies in technology but also from inadequacies in governance, processes and management. While the National Cyber Policy states that our mission is to build a secure and resilient cyber space for citizens, business and Government and to protect information and information infrastructure, build capabilities to prevent and respond to cyber threats, it has not specified how to achieve the objectives. To deal with the growing cyber threats we require an overarching national cyber strategy to prioritise the objectives in an evolving environment, achieve synergy between different institutions and work in coordination to deal with different threats particularly Tier V and VI threats. The cyber war is not merely a fiction. The DDOS attack in Estonia in 2007 is nicknamed as Web War I. In May 2009, North Korea was reported to have attacked all the web services of US Homeland Security and Transportation Departments and brought them down. Canada in 2009 suddenly discovered that Ghostnet had taken over 1300 Computers at various embassies around the World. This had the capability to turn on a computer's camera and microphone remotely without alerting the user and to export images and sound silently back to servers in China. These indicate the growing nature of cyber-attacks as also the fact that cyber space is becoming increasingly contested.

In view of the above when the cyber security threats are assuming dangerous dimensions, India has to evolve a national cyber strategy for defending its system by utilising optimally all its assets. This requires both defensive and offensive capabilities as also ability to detect the attackers. The offensive capability would be able to act as a deterrence to those who are working on Tier V and VI attacks. In short, India needs to have the concept of cyber–war deterrence as an essential part of its cyber strategy [4].

4. Threat from Chinese cyber hackers

China, with a colossal 640 million internet users, owns a large army of cyber security professionals, possesses extensive control over its internet, and employs patriotic and 'mercenary hackers' to confront its rivals including India. Chinese professional call 'network security' (*wangluo anquan*) what the world calls "cyber security". China achieved cyber security prowess early because Chinese computers themselves were under severe cyber espionage.

The Chinese Ministry of Public Security considers China as the largest victim of cyber-attacks and response to such attacks, Chinese experts felt, cannot be defensive. It is worth noting that China's warfare policy is based on what Mao Zedong called 'active defence' doctrine under which 'China strikes only after the enemy has struck, but will employ offensive operations at all levels of war and at all stages of conflict'.

Global cyber hackers targeted Chinese installations to which China had to retaliate and in the melee, India became a collateral Chinese target. China prepared its institutions and generals to not only counter cyber-attacks but also to adopt an offensive posture. The Chinese Academy of Military Sciences declared that an internet tornado had swept across the world

and Chinese military could not be passive in the internet war.
Soon Chinese hackers retaliated and hacked into Barack Obama's campaign computers in 2008. President Obama not only admitted the hacking of his computer data but informed that his rival John McCain's data were also stolen. The FBI detected the theft and warned both campaigns, which took some defensive steps. But what is nightmarish is: What would have happened had the Chinese hackers destroyed the data?
Media reports suggest that Chinese hackers targeted India's foreign and defence ministry's data. However, these are misleading reports since Chinese hackers are primarily trying to destabilize India's economy.
If Chinese hackers managed to destroy India's bank data, there would be financial chaos. As per the Reserve Bank of India, India's banking system is worth $190 billion, ranking it third largest among the BRICS countries and 15th in the world. A financial disruption wouldn't allow people to get their money, know whether they had it or if they had made payments. Money in the modern world is just an entry on a computer rather than gold and hard currency. Chinese hackers could ruin India without firing a single bullet. A rough estimation tells us that every year India is subjected to US$ 4 billion loss due to cyber attacks, a majority of which originates from China.
In its 2013 White Paper titled 'The Diversified Employment of China's Armed Forces', China reiterated its stand to protect its national security interests in outer space and cyberspace. The Chinese political leadership has taken direct charge of the country's cyber security as President Xi Jinping and Premier Li Keqiang have decided to head the Security and Informatization Leading Small Group, an exclusively network security structure. In 2014, while addressing the first meeting of the committee, President Xi Jinping clarified the importance of network security to the Chinese political agenda [5].

5. Cyber attacks and India's preparedness

Cyber warfare has been an issue for India for a long time now. In the recent years direct attacks has given way to cyber-attacks causing greater damage to India. This is complemented by adequate cyber security and lack of adequate infrastructure thus exposing India to a greater danger. Currently we do not have a cyber warfare policy and no concrete implementable cyber crisis management plan that can be deployed at the time of a cyber war [6].
In August 2010, the Indian government initiated the steps to strengthen the cyber security infrastructure in India. The strategy was directed to develop capabilities to snoop into network unfriendly countries, setup ethical hacking laboratories, state of the art testing facilities, develop counter measures for possible attacks and set up CERTs for several sectors. The strategy was a joint initiative National Technical Research Organization, the Defense Intelligence Agency, and the Defense Research and Development Organization. During this period, India discovered a Chinese variant of Stuxnet worm in Indian Installations. In addition to the Chinese worm, in December 2010, India's most secure website of India's Central Bureau of Investigation was defaced by Pakistan Cyber Army. This reinforced the need for a strong offensive and counter offensive capabilities and laws in cyber security.
The second cyber warfare conference, was held in November, 2011 which provided different aspects and case studies to showcase the current scenario and steps to increase the cyber security capabilities.
In October 2012, a government- private sector plan was setup under the guidance of Mr. Shivshankar Menon, National Security Advisor to Prime Minister Manmohan Singh. The purpose of the sector was beef up India's cyber security capabilities based on the recent attacks. Ironically, India faces a shortage of around 4.7 lakh experts in cyber security despite the country's reputation of being an IT and software powerhouse.
The new generation proxy war of Cyber warfare, can not only disrupt data-links, electronic devices and networks, but can also use to create panic at a greater extent. Platforms like social media can be used to reach out to maximum number of people in a fraction of second and spread mis-information. We have witnessed the panic caused by Social media in the mass exodus of people of North-East from Bengaluru, Hyderabad and Pune recently. The Pakistan Military Establishment, including ISI, is becoming impatient because of it's inability to create problems in Kashmir region and the lowering of intensity of insurgencies in the North-East.
In the past 65 years after independence, the Pakistan has lost major wars with India. Pakistan has realized that it can never defeat India in a direct war. The Pakistan Militia along with ISI started a proxy war in India consisting of trained Jihadi groups, whose purpose is to create havoc in India through various means. They were successful in creating some noise initially, but their recent efforts to spread terror has been foiled by the Indian Intelligence. Since the terror attacks are failing, Pakistan has started to use their jihadi groups to spread panic using Internet and social media. First, their websites pulled out photographs of violence and disasters from different countries, morphed and uploaded to show violence against Muslims in Myanmar and Assam. Second, they used SMS messages through their sleeper cells in India to circulate threat to all the North-East people working in major cities like Bengaluru, Hyderabad, Pune Delhi etc. The result was that there was mass exodus from these cities due to the threat posed in these messages.
Pakistan successfully used the next generation warfare, i.e. 'Cyber War' and managed to create a false perception of insecurity amongst the people from the northeast. The Indian intelligence agencies were clueless about it and the havoc was created by Pakistan using Cyber cells. The result was almost half a million people in panic left for their hometown in Assam. Although the Indian government raised protest with Pakistan, Pakistan denied all the allegations and asked for proof of the investigation.
The extent to which Cyber warfare can harm a country is unimaginable. Cyber warfare is not limited only to creating Havoc and spreading false information on Social media. At times of War, the adversary can easily manipulate the data, perception and decisions of the opponents. Aircrafts can be neutralized, Missiles can be caused to misfire to create destructions within. The country's transportation, banking system can be neutralized creating a havoc among the people [7].
Fake orders can be passed to military units including nuclear

strategic command. Television transponders can be hacked and forced to showcase fake news, creating further havoc in the country. Jamming of telephone lines, banks and financial institution will bring any country to the verge of bankruptcy. The only successful defense in case of a cyber warfare is powerful offence. The answer to defend our nation against cyber-attack does not lie in regulating Internet or banning social media as demanded by some. There is a need for strong Government policy to strengthen the country's defense against cyber war. India should setup a strong team of cyber Army to defend networks, data links and electronic devices and at the same time launch counter attack on the enemy. India is on the way of becoming the Silicon valley of the world and boasts a strong technically skills workforce who can be trained and utilized for this task [8].

6. Measures to thwart cyber attacks

India is likely to face increasingly sophisticated "destructive" cyber threats as compared to the "disruptive" attacks in the Indian cyberspace in the times to come. The government organizations — the Centre and states —are the main target of cyber-attacks, driven by motives ranging from theft, espionage and data extraction to counterfeiting. In 2015 and 2016, the government sector accounted for 27% and 29% of all cyber-attacks. We have to be prepared to thwart them effectively.

Other sectors high on the priority list of cyber criminals are banking, energy, telecom and defence, which along with the government, account for three-fourths of all cyber-attacks. The emergence of new services and apps, cloud and cognitive technologies, has made cyber security more challenging even as the value of data and its applications in commerce grows by the day, making cyber security a major task [9].

At present time in India, the development of cyber-assets depend upon how strong protection measure we have devised to protect it. It is the stage when cyber security should be placed at the zenith of priority even if it amounts to certain modifications and alterations in India's cyber domain. If the cyber security of the country is to be preserved the most pertinent consideration is that the security measures must be devised keeping in mind the native conditions and shall be developed by the Indian minds. This consideration again remind us the reason behind formal division of roles and responsibilities between the civil and military functions of cyber security.

As it is quoted by National Security Advisor Mr. S.S. Menon India needs to "harden its critical networks and develop metrics to certify and assure that our critical cyber networks, equipment and infrastructure are secure" and that "we must find ways to indigenously generate manpower, technologies and equipment that we require for our cyber security [10]."

7. Conclusion

India needs to prepare ground to tackle with the threats to cyber space and risks arising through cyber space, as a "step towards a coherent and comprehensive cyber security policy. Cyber space is developed as the platform of global governance and the problem of cyber security cannot be tackled by governments alone. Public Private Partnership (PPP) is required.

Even the prime Minister of India now acknowledged that India must be prepared to meet the challenges arising out of Internet and cyberspace.

In view of the above when the cyber security threats are assuming dangerous dimensions, India has to evolve a national cyber strategy for defending its system by utilising optimally all its assets. This requires both defensive and offensive capabilities as also ability to detect the attackers. The offensive capability would be able to act as a deterrence to those who are working on Tier V and VI attacks. In short, India needs to have the concept of cyber–war deterrence as an essential part of its cyber strategy.

8. References

1. Pradhan SD. Cyber security-need for an overall national cyber strategy, Chanakya Code, Times of India, 2016.
2. Kumar Davinder. India's Cyber Security: Architecture and Imperatives, India Foundation Journal, 2017.
3. Thakker Aman. 'It's Time for India to Update It's Cybersecurity Policy The Diplomat, 2017.
4. Pradhan SD. Chanakya Code, Times of India Blogs, 2016.
5. Lt. Gen. Gautam Banerjee. Dimensions of Cyber security in India, Vivekanand International Foundation, 2014.
6. Lt. Gen. Gautam Banerjee, 'Cyber warfare in Indian context, Vivekanand International Foundation, 2014.
7. Masood Ur. Rehman. Network Centric Warfare Capabilities in the Indian Military, South Asia Strategic Stability Institute, Weekly Pulse, Islamabad, 2012.
8. Staying safe in the Cyber world, Mass.gov blog, 24 Oct 2013, http://blog.mass.gov/blog/safety/staying-safe-in-the -cy ber-world/
9. Kumar Davinder, 2.
10. India's cyber security challenges, Institute of Defence Studies and Analyses Report, 2012.