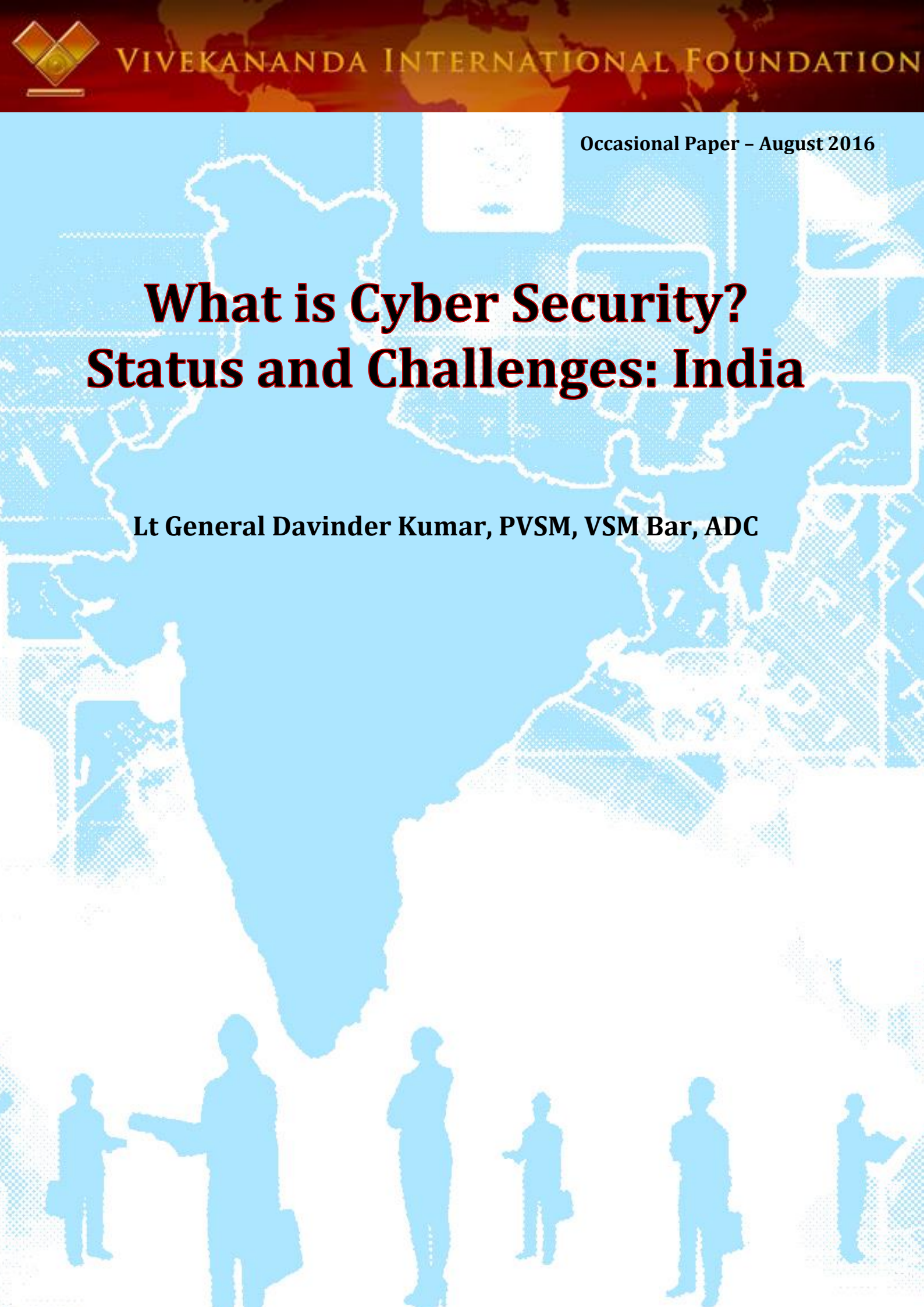
VIVEKANANDA INTERNATIONAL FOUNDATION

Occasional Paper – August 2016

What is Cyber Security? Status and Challenges: India

Lt General Davinder Kumar, PVSM, VSM Bar, ADC



About the Author

Lt General (Retd) Davinder Kumar is a scholar, soldier and a thinker. He retired as the ***Signal Officer-in-Chief of the Indian Army*** in September, 2006, after rendering 41 years of distinguished service. He was the ***CEO & Managing Director*** of ***Tata Advanced Systems Ltd,*** the *Tata's* lead vehicle in defence, aerospace, and homeland security from September, 2008 till September, 2011. As part of the high level negotiating team of the Tata Group, he successfully negotiated formulation of JVs with Sikorsky, Israel Aircraft Industries, AGT for homeland security and HELA for microwave components. He was instrumental in setting up the first helicopter cabin manufacturing facility in India from ground breaking to start of manufacturing in 159 days flat. He has been on the ***Board of Directors*** of both Public and Private sector companies and *Member of select Advisory body of Tata Group on Telecommunications and the Steering Committee on Defence of the Tata Group*

An Expert in the Net Work Centric, Information and Cyber Warfare, he was instrumental for the approval and setting up of the *Army Cyber Group* and the First *Information Warfare Brigade* of the Indian Army. He was the Project Director of Army Strategic Communication Network (ASCON) and is the author of the Defence Communication Network (1995), Tactical Communication System (1996), and ASTROIDS besides a number of regional optical fibre and satellite based networks in some of the most inhospitable terrains in the North and East India*. He headed the national study on Cryptography, was a member of the National Committee on spectrum management and Adviser on IT to the state of Madhya Pradesh*.

He has worked with *Indian Space Research Organisation* (*ISRO), Oil India*, and the *Planning Commission*. He has been an Examiner for the University Grants Commission, on the Court of The Indraprastha University, member of the *Hardware and Human Resource Groups of the IT Task Force* and the Advisory Committee of *National Disaster Management Authority* appointed by the Prime Minister. He was member of the committee which formulated the I T Act; 2000. He is a recipient of five National Awards including the highest for *Distinguished Service of the Most Exceptional Order.*

He also got the Best Engineer Award in 2005 and is the only serving officer to have been awarded the Fellowship of Indian National Academy of Engineering. He has over 400 papers to his credit and has also been invited to speak at various international fora like *RAND Corporation*, International Telecommunication Union (*ITU), World Battle Space Research Organisation*, *Brookings Institute, ASPEN Institute,* Wharton *University* and Centre for Strategic and International Studies, Beijing.

What is Cyber Security ? Status and Challenges: India

Rapid and unprecedented growth of Information and Communication Technology (ICT) and media with its all-pervasive penetration has ushered in the digital age. Not only has it brought the world together through globalisation, it has become the driver for economic growth. Technology and Information have become the new mantras of this digital transformation. We are witnessing a connected world with new business and cultural orientation. Business is being transacted at the speed of light with billions of dollars transferred every day across the globe. This transition from an industrial to an information era has created a new domain, "Cyberspace" and ushered in a new security paradigm with new threats to both national and human security. With large scale automation, rapid penetration of ICT and connectivity the developed nations are enjoying a much better quality of life that also makes them more vulnerable to cyber interventions. There exists a definite digital divide amongst the developed, developing and poor nations. This digital divide, coupled with the rising aspirations, easy access and low cost of ICT have created serious security issues wherein new threats by way of cyber-crime, cyber terrorism, cyber espionage and even cyber war have emerged making cyber security a strategic imperative at the national, regional and international levels.

Before we proceed further, it is necessary that we all are on the same page in as far as the terminology is concerned. There are no formal and internationally accepted definitions of terms like cyber space, cyber power, cyber warfare, cyber security and so on. However, definitions used by the U S of A are being used by most to comprehend these terms and their application. This should not inhibit the capacity building and application of "Cyber". There are no internationally accepted definitions of Air Power or Sea Power till date but that has not restricted their development and deployment as instruments of national power.

Definitions

Cyberspace

" A global domain, within the information environment, whose distinctive and unique character is framed by the use of electronics and electromagnetic spectrum

to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communication technologies ".[1]

Comments[2]

- Cyberspace is an operational space where humans and their organisations use the necessary technologies to create effects, whether solely in cyberspace or in and across the other operational domains and elements of power. It is an operational medium through which "strategic Influence" is conducted.
- The fundamental condition of cyberspace is the blending of electronics and electro-magnetic energy. The electronic technologies that we create and employ in cyberspace are the counterparts to vehicles, ships, aircrafts, missiles and satellites that we have created to exploit other domains.
- Cyberspace is used to create, store, modify, exchange and exploit information via electronic means.
- Networking of interdependent and interconnected networks using information communication technologies (ICT) are at the core of cyberspace capacity building that make it critical to national security and 21st century warfare capabilities.
- In the global economy of 21st century, cyberspace is perhaps the single most important factor linking all the players together, boosting productivity, opening new markets, and enabling management structures that are flatter yet with a far more extensive reach.
- Cyberspace is literally transforming how we create data itself, the raw material that fuels our economy and society.

Cyber Power[3]

"The ability to use cyberspace to create advantages and influence events in all the environments and across the instruments of power".

Comments

- While cyberspace is an "environment", cyber power is the "measure of the ability" to use and exploit that environment.
- Technology is a major factor since it determines the "ability to enter" cyberspace. The challenge is that the technology is constantly changing, and some users – nations, societies, non-state actors and the like; may be

[1] *From cyber space to cyber power by Daniel T Kuehl*
[2] *Ibid*
[3] *Securing Cyber space- a Global common, Presentation at VIF by Lt Gen Davinder Kumar*

able to leap over old technologies to deploy and use it to dramatic advantage. Obsolescence management and staying ahead of bad boys are the real challenges.

- Organisational factors play an important role for their mission; military, political or economic considerations would determine how cyber power is employed to impact and influence the elements of power.
- Cyberspace and cyber power are dimensions of "informational instrument" of power under the PIME (Political, Informational, Military, Economic) model.
- Cyber power is a crucial capability in the struggle of hearts, minds and ideas. It has an extensive impact on political, social and diplomatic affairs.
- Cyber power is an indispensable element of modern military capability across full spectrum of warfare from counter insurgency operations to nuclear warfare. Consequently, it is at the heart of new concepts and doctrines.
- Cyber power is shaping how governments connect with their citizens to provide services in ways that could not have been imagined a decade ago. It does the same for the development of new technologies; in their creation, exploitation and measurement of success.
- Cyber power demands and creates synergies across other elements and instruments of power and connects them in ways that improve all of them.

Cyber Security

Cyber Security, has been defined differently by different organisations. The International Telecommunication Union (ITU) has defined Cyber Security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets".[4] Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

[4] ITU-A Definition of Cyber Security www.Itu.Int

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

A simpler definition would be:

Cybersecurity refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals[5]

The Indian IT Act 2000 defines "Cyber Security" as means for protecting information, equipment, devices computer, computer resource, communication devices and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.[6]

Environmental Scan

India lives concurrently in three ages; Agrarian, Industrial and Information with varying coincidence amongst these depending on the induction and availability of technology, infrastructure, education and services. The Indian society is, therefore, in constant transition. While India has made considerable progress in the last decade or so towards the establishment of ICT infrastructure, enhancing the reach of the electronic media and extension of e-services in the finance, health and education sectors to ensure better governance, the development has been differential. There exists a digital divide wherein there is still a very large population who does not have the access to this digital world. The situation, however, is changing rapidly with the mobile telephone revolution which is under way and greater penetration of internet. India, with nearly a billion mobile telephones, has the second largest mobile subscriber base in the world. Thirty percent of these are smartphone users. India, at 375 million users (January 2016), again has the second largest number of internet users in the world with more than 30 percent in the rural areas. India has the largest undersea optical network. More than 90 percent of its population has access to TV which is transforming rapidly into a fully digital service.

[5] Webopedia. What is Cyber Security?

[6] *Indian IT Act 2000 as amended in 2008.*

Projects like National Broadband Network (Bharat Net), Digital India and 100 Smart Cities would change the digital landscape substantially with direct impact on security, governance, transparency and accountability.[7] 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 challenge 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 must ensure safe navigation through cyberspace – a global commons – for its prosperity and national security. It is absolutely imperative that security is built in ab-initio as an essential design parameter. Our thrust has to be towards "safe" infrastructure and facilities. We will have to adopt a "holistic approach" and ensure that the existing strategic inadequacies are overcome.

As India moves further into a digital world, she will become increasingly vulnerable to cyber interventions. The irony is that India has practically no technological, semi-conductor and electronic manufacturing base and limited human resource with skills particularly in system and large system integration. India announced her National Policy on Electronics one year before the National Cyber Security Policy in 2013. Unfortunately, there has hardly been any progress on ground. Consequently, technology, products, operating software, system engineers and integrators had to be imported with attendant impact on security, finance, dependency for maintenance and up gradation. In short, India has serious strategic inadequacies impacting on her "Technological Sovereignty". Implementation of NPE - 2012[8] concurrently with NCSP-2013[9] is an absolute pre-requisite. It is, in fact, at the very heart of Make in India Initiative.

The situation is of great concern with direct impact on human and National security, functionality and availability of critical infrastructure and governance. Ensuring comprehensive cyber security of our assets and National Information Infrastructure is thus both a national strategic imperative and an urgent national mission.

Threat Landscape

Cyber threat exists 24/7 and manifests along the full spectrum starting from cybercrime to cyber espionage to cyber terrorism and cyber war. The threat landscape is closely related to the growth of internet, progress of technology and

[7] *Telecom Statistics in India: Wikipedia*

[8] *National Policy of Electronics -2012*

[9] *National Cyber Security Policy -2013*

connectivity with other networks irrespective of their location. Initially, when computer software was written, some errors were accepted by design initially and then patched up subsequently. Network growth and connectivity propagated these "vulnerabilities". Some bad hats started exploitation of these for their personal gains. This was the genesis of cyber crimes. Over the period, the manufacturers became very cautious and protective measures like anti-virus vaccines and firewalls found their place in the networks and six sigma became the accepted standard for software. The decade 1980-90 was dominated by cyber crimes and corresponding protective measures. Both grew in their application, spread and sophistication in consonance with the growth of number of people connected and continue to do the same. About 80 percent of cyber interventions are related to cyber crime. The situation is going to become much worse as by 2020, the internet connections will far exceed the world population.

Technology, then facilitated unauthorized exfiltration of information and data stored in the networks. Accordingly, the decade 1990-2000 saw emergence of cyber espionage. Since then, cyber espionage has been accepted unofficially as permissible means for gathering intelligence with an exponential increase in technologies both for protection and stealing of information. Today, about 90 percent of intelligence is so obtained largely related to technology, finance and defence sectors. The latest is the collection of confidential information about people with the intention of its exploitation for financial gains, trolling, ransom and other cyber crimes.

The next technological event of stuxnet attack on the Iranian nuclear facility at Natanz was perhaps the most significant happening of the 21st century. It demonstrated the merger of the virtual and physical worlds. This has not only put the entire information infrastructure under threat with direct impact on public safety, national security and economic security but has heralded the arrival and efficacy of cyber weapons. Nations and societies will have to develop trusted and robust infrastructure with comprehensive plans for prevention, response and reconstitution. Recent attack on the German steel plant further reinforces this capability. The decade 2000 – 2010, can thus be seen when cyber attacks on physical infrastructure became a reality with attendant impact on both the human and national security.

An entirely new dimension has very recently been added by the hacking attack on the Sony Entertainment company, wherein for the first time, the information assets of the Corporate had been physically destroyed.[10]

Technology and feasibility of remote injunction of computer virus particularly through drones and aircrafts has totally eliminated the safety and security allegedly provided thus far by having an "air gap". This has raised the threat envelope by many notches and will have far reaching impact both in cyber terrorism and cyber war which will dominate the current decade. The USA had displayed EC -130 H aircraft on 23 September 2015, designed for integrated electronic and cyber warfare with the capability of injecting virus from air in the ground based networks. USA is reported to have dropped cyber bombs to neutralize ISIS networks and associated electronics.[11] **The threat increases exponentially when cyber and EW are employed in an integrated manner.**

The spread, reach and penetration of social media has brought to fore the threat of both social engineering and perception management and thus made available very inexpensive mechanism and capability for conducting Asymmetric warfare.

Threats in Near Future

In the next five years, the threat landscape is likely to change drastically with the emergence of virtual currency, digital economy, the Internet of Things (IoT), Dark web and the Outer net. **Nations and Societies will have to come together to fight these threats.**

To summarise, the threat landscape encompasses cyber crime, cyber espionage, cyber terrorism, social media and cyber war. This is so due to some unique characteristics of cyber space, namely

- offence dominance,
- difficulty in attribution of attacks thus providing anonymity to the attacker,
- Attack at the speed of light,
- An excellent tool for asymmetric warfare,
- No direct collateral damage and

[10] *"Hack Attack" by Davinder Kumar, Economic Times, 24 December 2014.*

[11] *Cyber bombing of ISI : Economic Times, 14 April 2016.*

- Relatively low cost of development of cyber weapons by states and non-state actors.

Militarization of cyberspace poses an ongoing threat. While more than 140 countries are busy developing cyber weapons, about 40 nations have some organization for both cyber security and cyber war in accordance with their respective cyber doctrines.

The US of A has promulgated its new military doctrine stating that cyberspace is the fifth domain – a new theatre of war. The applicability of international laws, in this domain, is still being debated. Nor is it possible to establish the start of a cyber war, since cyber weapons cannot be distinguished from normal cyber tools for hacking, frauds, and espionage. This ambiguity and uncertainty further compounds the threat.

Let us have a detailed look at each component of the threat spectrum.

Cyber Crimes

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyberspace and the worldwide web. It is a bigger risk now than ever before due to the sheer number of connected people and devices and increasing sophistication.[12]

According to United Nations Office on Drugs and Crime's (UNODC) Comprehensive Report on Cyber Crime (2013),[13] in 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60% of all internet users are in developing countries, with 45% of all internet users below the age of 25 years. By the year 2017, it is estimated that mobile broadband subscriptions will approach 70per cent of the world's total population. By the year 2020, the number of networked devices (the "internet of things") will outnumber people by six to one, transforming current conceptions of the internet. In the hyper-connected world of tomorrow, it will become hard to imagine a "computer crime," and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity

Cyber crimes are a real threat today and can be committed single handedly and do not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement

[12] *Cyber Crime by Clay Wilson*

[13] *Comprehensive Study of Cyber Crime, February 2013*

agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

Categories of Cyber Crime[14]

Cyber- crimes are broadly categorized into three categories, namely crime against:

- Individual
- Property and
- Government

Each category can use a variety of methods and they vary from one criminal to another.

Individual: This type of cyber- crime can be in the form of cyber stalking, distributing pornography or religiously sensitive material, trafficking, recruitment for unlawful activities including terrorism, propaganda and dissemination of offensive material. Such activities have a direct impact on "Human Security". Law enforcement agencies are taking this category of cyber- crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the real world. According to a Symantec report, India lost eight billion dollars to cyber crime related to finance alone, in 2013.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The

[14] *Categories of Cyber crime; Cyber Security- A Strategic Imperative for South Asia's Economic Development and Governance By Lieutenant General Davinder Kumar, PVSM, VSM Bar (Retd)*

perpetrators can be terrorist outfits, non-state actors or unfriendly governments of other nations.

Cybercrime: The facts

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker.
- Somebody's identity is stolen every 3 seconds as a result of cybercrime
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.

Types of Cyber Crimes[15]

There are many types of cyber- crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In developed nations, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organisations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software or exfiltrate technical designs and system parameters. This has become a major threat today. There are even peer sharing websites which encourage software piracy and many of these websites are now under surveillance of the security agencies. Many nations have promulgated laws to address these cyber- crimes and prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and e-mails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

[15] ***Cyber Security and Related Issues: Comprehensive Coverage.*** *Y INSIGHTS · NOVEMBER 25, 2014*

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber- crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history. What is of greater concern is the use of your identity for illegal activities like terrorism and drug trafficking.

Child Soliciting and Abuse: This is a very serious cyber- crime wherein criminals solicit minors via chat rooms for the purpose of child pornography or even kidnapping. Security agencies carry out regular monitoring of chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

Malicious Software (Malware): These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system. Computer viruses, worms and Trojans form part of Malware.

Examples: Major International Crimes

Hackers steal £650m (16 Feb 2015)-Cyber Heat[16]

British banks are thought to have lost tens of millions of pounds after a gang of Russia based hackers spent the last two years orchestrating the largest cybercrime ever uncovered. As much as £650 million is thought to have gone missing after the gang used computer viruses to infect networks in more than 100 financial institutions worldwide. The hackers managed to infiltrate the bank's internal computer systems using malware, which lurked in the networks for months, gathering information and feeding it back to the gang. The illegal software was so sophisticated that it allowed the criminals to view video feeds from within supposedly secure offices as they gathered the data they needed to steal. Once they were ready to strike, they were able to impersonate bank staff online in order to transfer millions of pounds into dummy accounts. They were even able to instruct cash machines to dispense money at random times of the day even without a bank card.

[16] ***Hackers steal £650 million in world's biggest bank raid ... (www.telegraph.co.uk › News › UK News › Crime)***

While the criminals behind the audacious electronic raid are thought to be based in Russia, the scale of their crime was truly global with banks in Japan, China, and the United States and throughout Europe having been hit.

Attack on Sony Play Stations[17]

Given the plethora of sensitive information they house, gaming networks are a common target for cybercriminals. The most alarming of which occurred in 2011. After an external breach, no less than 77 million accounts filled with passwords, names and address were compromised. Foolishly, Sony had left much of their customer's details unencrypted, exposed to the pitfalls of cyber theft. Sony also confirmed that some user's credit card details, which were encrypted, were also at risk.

The attack, occurring between 17th and 19th of April, forced Sony to switch off their PlayStation Network and music service Qriocity. The outage prevented any play station (PS3 or PSP) owner from accessing online content, and lasted for a total of 23 days. Sony announced shortly after that damages tallied up to $171 million (£115 million).

Attack on Nasdaq[18]

Before being chipped down to number two by "Cyber Heat" above, the notorious accolade of "World's greatest cybercrime" was held by an altogether different fivesome. Those pesky Russians were at it again though, with four of them joined by a Ukrainian named Mikhail Rytikov. Initially targeting large retailers such as 7–Eleven Inc. and Carrefour SA, the group eventually headed for financial corporation Nasdaq.

Using specially designed sniffer programmes, the hackers were able to target credit card information as it was processed between companies. In a statement made at the culprit's case, US attorney Paul Fishman said: "the five conspired in a worldwide scheme that targeted major corporate networks, stole more than 160 million credit card numbers and resulted in hundreds of millions of dollars in losses,"

In total, those losses amounted to $300 million (£202 million).

[17] 2011 Play station network outage; *Wikipedia the free encyclopedia.*

[18] *The Business Insider; The Massive Hack Of The Nasdaq That Has Wall Street Terrified of Cyber Attacks;* STEPHANIE YANG,ELENA HOLODNY0 JUL 18, 2014,

Ashley Madison Data Breach[19]

In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The group copied personal information about the site's user base and threatened to release users' names and personally identifying information if Ashley Madison was not immediately shut down. On 18 and 20 August, the group leaked more than 25 gigabytes of company data, including user details.

Because of the site's policy of not deleting users' personal information – including real names, home addresses, search history and credit card transaction records – many users feared being publicly shamed.

Following the hack, communities of Internet vigilantes began combing through to find famous individuals, who they planned to publicly humiliate. France reported that 1,200 Saudi Arabian .sa email addresses were in the leaked database, and in Saudi Arabia adultery can be punished with death. Several thousand U.S. .mil and .gov email addresses were registered on the site. In the days following the breach, extortionists began targeting people whose details were included in the leak. One company started offering a "search engine" where people could type email addresses of colleagues or their spouse into the website, and if the email address was on the database leak, then the company would send them letters threatening that their details were to be exposed unless they paid money to the company.

Office of Personnel Management Data Breach[20]

In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people. Later, FBI Director James Comey put the number at 18 million. The data breach, which had started in March 2014, and may have started earlier, was noticed by the OPM in April 2015. It has been described by federal officials as among the largest breaches of government data in the history of the United States. Information targeted in the breach included personally identifiable information such as Social Security numbers, as well as names, dates and places of birth, and addresses. The hack went deeper than initially believed and likely involved theft of detailed security-clearance-related background information.

On July 9, 2015, the estimate of the number of stolen records had increased to 21.5 million. This included records of people who had undergone background checks, but

[19] ***Hackers Finally Post Stolen Ashley Madison Data | WIRED***
www.wired.com/.../happened-hackers-posted-stolen-ashley-madison-data...,Aug 18, 2015.

[20] *Wikipedia, the free encyclopedia*

who were not necessarily current or former government employees. Soon after, Katherine Archuleta, the director of OPM, and former National Political Director for Barack Obama's 2012 re-election campaign, resigned.

Cyber Espionage

There is no standard definition of cyber espionage. Wikipedia defines it as "The act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in faraway countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers".[21]

Cyber spying typically involves the use of such access to secrets and classified information or control of individual computers or whole networks for a strategic advantage and for psychological, political and physical subversion activities and sabotage. More recently, cyber spying also involves analysis of public activity on social networking sites like Facebook and Twitter.

Mc Fee-sponsored report produced by Centre for Strategic and International Studies (CSIS) called, "The Economic Costs of Cyber Attacks and Cyber Espionage"[22] reveals the cost of cyber crime and espionage racks up between US $300 billion to $1 trillion. These costs are likely to increase with the greater internet penetration, and as organizations continue digitalizing their products to compete in ever more competitive markets. The report also indicates no less than 508,000 US jobs alone are potentially lost each year due to cyber espionage.

The Internet is an immense gift to spies. Information that once required physical access or recruitment of agents can now be downloaded from afar. China has a domestic communications intelligence program called "Golden Shield" that uses new technologies to monitor domestic internet; it is likely that technologies developed for Golden Shield are also used for foreign intelligence collection. China's military is

[21] *Cyber Espionage; Wikipedia, the free encyclopedia.*

[22] *Centre of Security and International Studies (CSIS); "The Economic costs of Cyber Attacks and Cyber Espionage" Mc fee report.*

copying the U.S. military and developing 'computer network operations' to attack U.S. information resource and, perhaps, infrastructure in the event of a conflict. Russia, France, Israel and others, even North Korea, have similar programs. But perhaps except in a conflict scenario, the last thing that an intelligence service that had successfully penetrated an opponent's networks would want is to be noticed. The goals are either to get in, collect data, and send it out unobserved or to sit there unobtrusively. In either case, if someone stumbles across the effort, you will want to have covered your tracks well enough that blame cannot be ascribed.

The ease of computer espionage puts a heavy burden on defense. Networks will be vulnerable for a long time. There is an immense quantity of valuable data on open systems, particularly in government research facilities and in the private sector. We should assume that those who want it have already downloaded much of this stored data.

A skilled virtual community of cybercriminals has grown up in the last few years, trading tools, renting compromised networks and hiring out for attacks. The easily accessible tools give hackers capabilities that were available only to the larger intelligence services a few years ago, and work in the Intelligence community concludes that large multinational corporations could, if they wished, purchase intelligence capabilities as good as or better than those fielded by a medium sized country. Unlike the bored teenagers, today's hackers include professional criminals whose goal is not excitement but money. These cybercriminals might steal data for their own purposes, at the behest of an intelligence service, or even under contract to a business competitor.

Nations, Industry and organisations across the world are involved in cyber espionage. It is estimated that more than 90 percent of "open source intelligence" is being obtained from the cyber world. It is economical, quick and safe.

Cyber espionage is also being used for technology theft and for launching probing missions on the critical infrastructure for possible exploitation later. Internet has thus become a very powerful source for intelligence collection in support of national diplomatic, military or economic objective. What makes cyber espionage a more serious threat is the fact that "Attack Vectors" for both cyber espionage and cyber attack are the same[23]

[23] *Cyber espionage--Computer Espionage, Titan Rain and China James A. Lewis CSIS*

So serious is the economic cost and the threat to national security due to cyber espionage that during the recent summit meeting of President Obama and Xi Jinping, the USA allegedly had to threaten economic sanctions on China to get the mutual agreement signed which prohibits "Economic Espionage" by both nations.[24]

Important Incidents of Cyber Espionage World wide

- The Cuckoo's Egg,[25] published in 1989 by Cliff Stoll, tells the story of how an Eastern bloc service (probably the KGB) hired a group of West German hackers to steal data from U.S. military computers. The West Germans connected remotely to university networks in the U.S. and used them for the attacks. When the West Germans were finally tracked down and arrested, they did not know who had commissioned them!

- **Titan Rain**[26] was the designation given by the federal government of the United States to a series of coordinated attacks on American computer systems since 2003; they were known to have been ongoing for at least three years. The attacks were labeled as Chinese in origin, although their precise nature, e.g., state-sponsored espionage, corporate espionage, or random hacker attacks, and their real identities – masked by proxy, zombie computer, spyware/virus infected – remain unknown. The activity known as "Titan Rain" is believed to be associated with an Advanced Persistent Threat. The attacks were "most likely the result of Chinese military hackers attempting to gather information on U.S. systems. Titan Rain hackers gained access to many United States defense contractor computer networks who were targeted for their sensitive information, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

- In March 2009, a global cyberespionage network named GhostNet[27] was revealed, which exploited a known vulnerability in Adobe PDF reader. GhostNet spied on multiple high-value targets like ministries of foreign affairs, embassies etc. in 103 countries, international organizations, news

[24] *US and China Reach Historic Agreement on Economic ...*
*www.wired.com/.../us-china-reach-historic-**agreement-economic-espiona**...*
[25] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[26] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[27] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*

media and NGOs. Most attacks under GhostNet originated in China, though involvement of the Chinese government was not ascertained.

- In April 2009, hackers stole terabytes of data related to design and electronics systems of the F-35 Lightning II fighter jet.[28] The sensitive data was encrypted before exfiltration to sources in China, making it impossible to determine precisely what information was stolen.
- In April 2010, computer systems of the Indian Defense Ministry and Indian embassies in various countries were compromised.[29] Attacks stole classified information including designs of weapon systems, internal security assessments of sensitive regions and emails from Dalai Lama's office. The attacks were traced back to China.
- In April 2011, within a month of the RSA breach, the stolen SecurID tokens were used to hack defense contractor L-3 Communications for theft of sensitive information.[30]
- In May 2011, Lockheed Martin as well as Northrop Grumman were targeted in a cyberattack using the stolen RSA SecurID tokens, though the attacks were thwarted.[31]
- In July 2011, unknown attackers breached Pentagon networks stealing 24,000 files, with the exact damage being undisclosed.[32]
- In August 2011, Operation Shady Rat[33] was revealed to have been attacking 70 corporations and government organizations in the US since mid-2006 and other international targets. This cyber-espionage campaign employed spear-phishing with attached files containing malware that exploited a known vulnerability in Microsoft Excel to open a backdoor.
- In October 2011, two US satellites[34] were interfered with for few minutes, allegedly by attackers from China.

[28] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[29] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[30] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[31] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[32] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[33] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[34] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*

- In September 2012, the White House became a victim of spear-phishing attacks allegedly carried out by hackers in China.[35]
- In December 2012, computer networks of Indian government were breached, compromising 10,000 email accounts[36] of top government officials and information on troop deployment.
- In February 2013, a US government report revealed that 23 US gas companies were targeted by cyberattacks that stole potentially security-sensitive information.[37]
- In May, infiltration of systems at defense contractor QinetiQ by Chinese hackers was discovered. The attackers were in the system since 2007 because of a known security flaw resulting in the compromise and exfiltration of most of the company's research.[38]
- Also in May, a report by the Defense Science Board reported that designs of US defense systems including the Patriot missile system (PAC-3), Terminal High Altitude Area Defense and Navy's Aegis ballistic-missile defense system had been compromised by persistent, highly-sophisticated cyberattacks carried out by China.[39]
- In August 2013, hackers gained access to personal information, social security numbers and payroll information of 14,000 current and former employees at the US Department of Energy.[40]
- In September 2013, Operation Kimsuky[41] was revealed to be spying and stealing information from South Korean think-tank organizations using malware, delivered via a spear-phishing campaign. North Korea was blamed for the targeted attack as the malware specifically disabled a particular South Korean antivirus.
- In the past year alone, the number of cyberattacks worldwide grew by 48 percent and the cost of each incident increased 92 percent. Hackers attacked "Target Enterprise" in January 2014 and stole credit card information from

[35] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[36] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[37] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[38] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[39] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[40] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*
[41] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University. Page 5*

more than forty million customers, which they sold on the black market for $53.7 million.[42]

- An attack on JPMorgan Chase went unnoticed for two months—despite the company's $250 million cybersecurity budget—affecting seventy-six million households and seven million businesses.[43]
- And in 2014, both the White House and State Department announced breaches, likely carried out by Russian-backed hackers.[44]

Global Cyber-espionage Campaigns[45]

- In October 2011, it was reported that 760 organizations worldwide have been under attack by a cyber-espionage campaign stealing sensitive information.
- In January 2013, another global malware campaign, called Red October was exposed and is believed to have been active since May 2007. The campaign exploited vulnerabilities in Java, Microsoft Excel and Word software for stealing information from governments, embassies, research institutions, organization in trade and commerce, nuclear/energy research, oil and gas, aerospace and military sectors.
- In June 2013, cyber-espionage campaign named NetTraveler, allegedly by China, was discovered with victims across multiple sectors including government institutions, embassies, oil and gas industry, research institutes, military contractors and activists in 40 countries.
- In September 2013, another cyber-espionage campaign, Operation IceFrog, was revealed. It had attacked military, shipbuilding, maritime operations, research companies, telecom operators, satellite operators, mass media and television organizations in South Korea and Japan. The malware exploited known vulnerabilities and hijacked sensitive documents and credentials for accessing internal networks.

Cyber Terrorism:[46]

Although there are a number of definitions which describe the term terrorism, one of the definitions that are frequently encountered is that terrorism is "the unlawful use or threatening use of force or violence by a person or an organized group against people or property with the intention of intimidating or forcing societies or

[42] *Presentation on Cyber Security at Quad conference, Jaipur by Lt Gen Davinder Kumar*
[43] *Ibid*
[44] *Ibid*
[45] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University, Page 9*
[46] *CYBER TERRORISM– GLOBAL SECURITY THREAT - Mitko Bogdanoski*

governments often for ideological or political reasons." Interactions between human motives and information technology for terrorist activities in cyberspace or in the virtual world can be addressed as cyber terrorism.[47] This threat can manifest itself in many ways, such as hacking computer systems, programming viruses and worms, Web pages attack, conducting denial of service (DoS) attacks, or conducting terrorist attacks through electronic communications on critical information infrastructure.

Considering the fact that the terrorists have limited funds, cyber attacks are increasingly attractive, because, their implementation requires a smaller number of people and certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to remain unknown, because they can be very far from the place where the act of terrorism is committed. Unlike the terrorists that place their camps in countries with weak governance, cyber terrorists can store anywhere and remain anonymous.

There are huge possibilities of conducting cyber terrorism through Internet using advanced technology. Possible targets of cyber terrorism can be considered government computer networks, financial networks, traffic control, power plants, telecommunication networks, health facilities etc The reason for this is that the terrorists identifies all the above as most suitable targets to be damaged or put out of operation in order to cause chaos and gain publicity.

Systems manipulation through "secret entrance" software, stealing classified information, data deletion, Web sites damaging, viruses inserting, etc. are just a few examples of how terrorists can enter into the secured system. The terrorist attacks enabled by computer technology can be also conducted through the air traffic control system or by remote damage of the power supply networks. The new information technologies (IT) and the Internet are more often used by terrorist organizations in conducting of their plans to raise the financial funds, distribute their propaganda and secure communications. The terrorist organizations also use the Internet to "reach out" to their audience, without need to use other media such as radio, television or holding various press conferences.

Cyber terrorism attacks can occur in two forms, one used to attack data, and others focused on control systems. Data theft and destruction leads to service sabotage and this is the most common form of Internet and computer attacks. The attacks focused on the control systems are used to disable or manipulate the physical

[47] *Ibid*

infrastructure.[48] Central to this is the ability to exploit the vulnerabilities. This is accomplished by sending data over the Internet or by penetrating security systems.

Some Examples/Incidents[49]

- In March 2000, a disgruntled employee used the internet to slip one million liters of unprocessed sewage into the river and coastal waters in Queensland. He achieved this on the 45th attempt by manipulation of control system. Earlier 44 unsuccessful attempts were not detected.
- In 1988, a terrorist guerrilla organization, flooded embassies of Sri Lanka with 800 email-s a day. The message which was appearing was "We are the Internet Black Tigers and we are doing this to disrupt your communications." Department of Intelligence characterizes the attack as the first known terrorist attack on government computer systems.
- Internet saboteurs in 1998 attacked Web site of the Indian Bhabha Atomic Re-search Centre and stole e-mails from the same center. The three anonymous saboteurs through online interview claimed that they protest against recent nuclear explosions in India.
- In July 1997, the leader of the Chinese hacker group claimed that temporarily disallowed Chinese satellite and announced that hackers set up a new global organization to protest and prevent investment by Western countries in China.
- In September 1998, on the eve of parliamentary elections in Sweden, saboteurs attack the Web site of the right-wing political party in Sweden and created a link to a Web site on the left and to the pornographic sites. The same month, saboteurs attacked the website of the Mexican government in protest against government corruption and censorship.
- Romanian hackers on one occasion managed to intrude into the computer systems controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. Fortunately, their activity is stopped before any accident occurred.

[48] *Ibid*

[49] *2001-2013: Survey and Analysis of Major Cyberattacks Tavish Vaidya Georgetown University*

- During the Kosovo conflict, Belgrade hackers conducted a denial of service attack (DoS) on the NATO servers..
- During the Palestinian-Israeli cyber war in 2000 similar attack had been used. Pro-Palestinian hackers used DoS tools to attack Israel's ISP (Internet Service Provider), Netvision. Although the attack was initially successful, Netvision managed to resist subsequent attacks by increasing its safety.
- Also in April 2007, numerous journalistic organizations associated with the "Associated Press" reported that cyber attacks on critical information infrastructure on Estonia is conducted by computer servers located in Russia, although it was later determined that it is a Distributed DoS attacks carried out by different locations around the world (U.S., Canada, Brazil, Vietnam and other locations).

Analysts point out these crime examples as low level information warfare.

National power grids hit by cyber terrorist onslaught (07/04/2015).[50] An analysis of federal energy records has revealed that parts of the US power grid are attacked online or in person every few days. This threat is now also looming over major cities outside the US such as London.

There are now growing fears on both sides of the Atlantic that terrorist groups or hostile governments might be behind the repeated attempts to hack into the power grids' control systems. Other possibilities include that of an organised criminal gang (OCG) using the threat of repeated power outages to hold a city such as New York or London to ransom.

A group of terrorist hackers located in Iran called **Parastoo** is already known to be actively recruiting software engineers with precisely those skills needed to bring down the power supply in a major city such as New York or London. Parastoo has already been linked to a military-style attack on an electric power station, the PG&E Metcalf substation in California on 16 April 2013. Parastoo now claims it has been testing national critical infrastructure using cyber vectors.

[50] *National power grids hit by cyber terrorist onslaught 07/04/2015*
http://www.itproportal.com/2015/04/07/cyber-terrorists-target-national-power-grids/#ixzz45niOuKZ3

Social Media

"We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."[51]

Social Media like Face Book, Twitter, You tube, weblogs and LinkedIn have emerged as very powerful tools for perception management, social engineering and Open Source Intelligence. It is being exploited by the super powers and the poor/developing nations equally. It is a double edged weapon which can also be used by the Government. It has emerged as a major instrument of waging "Asymmetric Warfare" through exploitation of the aspirations of people, differential development, varying religious beliefs and cultural leanings. These have also become attractive sources for recruitment and radicalisation by the terrorist organizations. More importantly, social media is a technological innovation both for change and governance. It has promoted "citizen journalism" that characterizes the news today.

Nations across the world are putting legal frame work, infrastructure and human resource for monitoring this media to remain proactive. Major issues are Privacy vs human/national security.

Two recent examples of impact of social media is the "Arab Spring" of 2011 and the mass exodus of students from the North-East from Bengluru and other cities due to rumours sent as text messages initially and subsequently on twitter and face book. As far as India is concerned, social media provides the biggest challenge and an opportunity. This needs to be managed to ensure national and individual security and exploited for good governance.

Cyber Warfare

It is universally acknowledged that the 21st century war will be highly "Cyber-centric" if not fully led by cyber theatre. Glimpses of these have been given by the Russian assault on Estonia and Ukraine. While in Estonia, it was pure cyber intervention, in Ukraine, it was a combination of cyber and Kinetic attacks wherein the bits preceded the bullets. This operation is a land mark in Cyber Enabled Warfare.

Cyber space has been accepted as the fifth domain of war that nations need to protect and exploit for offensive operations. Militarisation of cyberspace, and

[51] Reference Social Media-A New Strategic Weapon by Lt Gen Davinder Kumar

development of cyber weapons are raising the spectre of cyber war. Cyber weapons are being equated with nuclear weapons and are being termed as, "Weapons of Mass Disruption". Strategic thinkers are debating issues like, "Cyber Deterrence".

Military planners across the globe are at inflexion point taking far reaching decisions which include the ushering in of cyber weapons fully integrated into military operations and kinetic warfare. Nations like USA, Russia, China and UK have already pronounced their respective Cyber warfare doctrines, created appropriate organisations and polices to implement the same and tested cyber weapons on a limited scale[52]. As per a report appearing in the Times of India on 15 April, the USA is dropping "Cyber Bombs" as part of its operations against the ISIS.[53]

The Pentagon has recently issued a tender valued at 460 million dollars for design and delivery of cyber bombs.[54]

China has developed "Full Spectrum" capabilities in cyber warfare, has recently announced a major organisational transformation and integrated kinetic and information warfare in accordance with her National Doctrine. She has a powerful "cyber militia" which can operate both as non-state actors and as part of state machinery. Chinese cyber capabilities will have to be factored in any decisions or policy formulations made by India.[55]

Insider Threat

Insider threat and non- state actors represent extreme threats. There is no defence against a fifth columnist. Their involvement in any major cyber attack or intervention is almost certain for either technical or human intelligence.

Threats in Technical Domain and Attack Vectors/Profiles[56]

We have had a look at the "Threats in Physical Domain" and how these have escalated over a period in consonance with technological developments. However, actual cyber interventions happen by exploiting Threats in Technical domain either

[52] *VIF report on National Cyber Commission*

[53] *USA Dropping Cyber Bombs on ISIS.* https://defensesystems.com/articles/2016/02/29/dod-carter-isis-cyber-bombs.aspx

[54] *The Secret Pentagon Push for Cyber Weapons, November 5, 2015, Aliya Stretsen*

[55] *Cyber Capability of China- a paper by Lt Gen Davinder Kumar for USI*

[56] *ENISA Threat Landscape ENISA Threat Landscape 2013 - Europawww.enisa.europa.eu/...threat...threat...2013...emerging-cyber-threats/.../...*

as Attack Vectors or as the means/tools for cyber-attacks. Some of the prominent Threats in Technical Domain are listed below along with the Current Trends.

- **Hacking/Cracking**
  Hacking in simple terms means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer.

- **Drive-by Exploits**
  This threat refers to the injection of malicious code in HTML code of websites that exploits vulnerabilities in user web browsers. Also known as drive-by download attacks, these attacks target software residing in Internet user computers (web browser, browser plug-ins and operating system) and infects them automatically when visiting a drive-by download website, without any user interaction. Current Trend—Increasing.

  Worms/Trojans
  Worms are malicious programs that have the ability to replicate and re-distribute themselves by exploiting vulnerabilities of their target systems. On the other hand, Trojans are malicious programs that are stealthily injected in user's systems and can have backdoor capabilities (Remote Access Trojans - RATs) or steal user data and credentials. Both worms and Trojans are two classic types of malware being widespread in cyberspace. Current Trend ---- Stable

- **Code Injection Attacks**
  This threat category includes well-known attack techniques against web applications such as SQL injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. The adversaries placing such attacks try to extract data, steal credentials, take control of the targeted webserver or promote their malicious activities by exploiting vulnerabilities of web applications. Current Trend—Increasing.

- **Exploit Kits**
  Exploit kits are ready-to-use software packages that "automate" cybercrime. They use mostly "drive-by download attacks" whose malicious code is injected in compromised websites. These attacks exploit multiple vulnerabilities in browsers and browser plug-ins. Moreover, exploit kits use a

plethora of channels to deliver malware and infect unsuspected web users. An important characteristic of exploit kits is their ease of use (usually through a web interface) allowing people without technical knowledge to purchase and easily use them. Current Trend—Increasing

- **Botnets**
  A Botnet is a set of compromised computers which are under control of an attacker. These compromised systems are called bots (or 'zombies') and they communicate with the bot master that can maliciously direct them. Botnets are multiple usage tools that can be used for spamming, identity theft as well as for infecting other systems and distribute malware. Current Trend – Stable

- **Denial of Service**
  A denial-of-service attack (DoS) is an attempt to make a resource unavailable to its users. A distributed denial-of-service attack (DDoS) occurs when multiple attackers launch simultaneous DoS attacks against a single target. In DDoS attacks, attackers use as much firepower as possible (usually through compromised computer systems/botnets) in order to make the attack difficult to defend. The perpetrators of DoS attacks usually either target high profile websites/services or use these attacks as part of bigger ones in order achieve their malicious goals. As stated, despite the fact that these kinds of attacks do not target directly the confidentiality or integrity of the information resources of a target, they can result in significant financial and reputation loss. Current Trend—Stable

- **Phishing and Spear Phishing**
  Phishing is the combined use of fraudulent e-mails and legitimate looking websites by cybercriminals in order to deceitfully gain user credentials. Phishers use various social engineering techniques to lure their victims into providing information such as passwords and credit card numbers. Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC. Current Trend – Stable.

Compromising Confidential Information

Compromising of confidential information refers to data breaches that occurred via intentional, unintentional information disclosure performed by

internal or external threat agents. This threat targets sensitive information from various sectors such as public health sector, governmental organizations, small-medium businesses (SMBs), large organizations etc. Data breaches are usually realised through some form of hacking, incorporated malware, physical attacks, social engineering attacks and misuse of privileges. Current Trend- Increasing.

- **Rogue- ware/Scareware**
  The Rogue- ware threat consists of any kind of fake software that cybercriminals distribute (e.g. via social engineering techniques) in order to lure users to their malicious intentions. A more specific kind of rogue-ware is scareware, a rogue security software, which tries to infect computers by providing fake security alerts. Current Trend- Stable.

- **Spam**
  Spam is the abusive use of e-mail technology to flood user mailboxes with unsolicited messages. Adversaries using this threat, force the e-mail messages to be received by mail recipients. Spam activity costs very little to the sender; on the other hand it is time consuming for recipients of spam messages and costly in terms of resources (network and storage) for service providers, Current Trend—Decreasing.

Targeted Attacks

A targeted attack occurs when attackers target a specific entity/organization over a long time span. Often the objective of targeted attacks is either data exfiltration or gaining persistent access and control of the target system. This kind of attack consists of an information gathering phase and the use of advanced techniques to fulfil the attacker's goals. The first phase can possibly involve specially crafted e-mails (spear phishing), infected media and social engineering techniques, whereas the second phase involves advanced and sophisticated exploitation techniques. Current Trend- Increasing.

Identity Theft

In a networked world, the identity of a user is the unique piece of information that makes this specific user distinguishable. This information is usually a pair of credentials (username/password) or other confidential information such as Social Security Number (SSN) or credit card number. Identity theft is an attack that occurs when an adversary steals user credentials and uses

them order to serve malicious goals, mostly related with financial fraud. Current Trend—Increasing

- **Rogue Certificates**
  Digital certificates are a means of defining trust in Internet. Attackers steal, produce and circulate rogue certificates which break the aforementioned chain of trust, giving them the capability of engaging in attacks that are undetectable for end users. By using rogue certificates, attackers can successfully run large scale man-in-the-middle attacks. Moreover, rogue certificates can be used to sign malware that will appear as legitimate and can evade detection mechanisms. Current Trend – Increasing.

- **Advanced Persistent Threat (APT)**
  An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. Current Trend – Increasing

- **Zero-Day Vulnerability**
  A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Current Trend – Stable.

- **Cyber Stalking**
  This term is used to refer to the use of the internet, e-mail, or other electronic communications devices to stalk another person. Cyber stalking can be defined as the repeated acts of harassment or threatening behaviour of the cyber-criminal towards the victim by using internet services. Trend – Stable

- **Spyware**
  Spyware invades a computer and, as its name implies, monitors a user's activities without consent. Spywares are usually forwarded through unsuspecting e-mails with bonafide e-mail identities. Spyware continues to infect millions of computers globally. Trend – Increasing.

- **Data Diddling**[57]
  Usually done in conjunction with data interception, valid data intended for a recipient is hijacked or intercepted and then is replaced with an erroneous one. This could also apply to illegal tapping into database and altering its contents. Basically, any form of alteration without appropriate authorization falls under this category.

  Ransomware[58]

  It is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan whose payload is disguised as a seemingly legitimate file; thus, Ransomware is an access-denial type of attack that prevents legitimate users from accessing files.

Current Cyber Security Scenario: India

Cyber threats are no less a nightmare for the Indian government than terrorist attacks as it embarks on ambitious and high-profile projects such as Digital India'

According to Symantec's Annual Internet Security Threat Report 2015,[59]

- There has been an increase in targeted attacks on industries dealing with critical infrastructure in India in 2014.
- The year also saw 317 million malware variants globally or nearly 1 million new malware daily.
- There has also been an increase in targeted attacks in businesses dealing with critical infrastructure particularly in financial sector, communication, transportation – thus underpinning the national security and economy. Among these attacks, 60 percent were on large enterprises.
- In terms of ranking, India comes in third in the global threat rank by source; 3.95 percent of malicious activity in the overall percentage is detected here.

[57] ***Cyber Security and Related Issues: Comprehensive Coverage.*** *Y INSIGHTS · November 25, 2014 .*
[58] *Ransomware; Wikipedia the free encyclopedia*
[59] *Symantec's annual Internet Security Threat Report, 2015*

- India ranks No. 1 when it comes to number of social media scams in the Asia Pacific Japan (APJ) region, and No.2 globally. This is also an indicator of a population that actively uses internet and social media and the mobile penetration.
- Social media scams through manual sharing accounted to over 80 percent of the overall social scams in India.
- The country was reported with the third highest number of ransomware attacks in Asia with over 60,000 attacks per year/170 attacks per day/7 attacks per hour.
- According to CERT-IN, by June 2013, 42 lakh computer systems including mobile phones were infected in India with Botnet virus.[60]
- Thanks to botnet viruses of the kind CUTWAIL, India is the leading generator of spam in the world.
- India figures third in the list of countries targeted by phishing attacks with more than 23% of online users facing these attacks in 2014. So, there is a huge possibility that by mistake employees could be revealing crucial information to the rivals. Employees would be unable to differentiate phishing emails from legitimate ones.
- **Ramnit Botnet** virus infected about 3.2 million computers across the world and has been in existence for nearly five years. The worst affected countries in recent times have been India with27 percent, Indonesia with 18 percent, Vietnam with 12 percent and Bangladesh with 9 percent.
- India has the third largest infected computers with Zero Access botnet virus. It is a sophisticated, very virulent and resilient botnet active since 2011.
- While threat landscape knows no border and is a global concern -- considering that threats can come from anywhere, the law enforcement is one of the biggest concerns in India.

The threat landscape needs to be analyzed carefully –- we have everything now from individual hackers, to hacktivists, to basic cyber criminals to organised crime groups, non-state actors, all the way up to national/state sponsored attacks. Looking

[60] *CHALLENGES AND PROSPECTS OF CYBER SECURITY IN INDIAN CONTEXT (USI: 20 May, 2015) By Lt Gen Davinder Kumar.*

at this varied spectrum, there will be a lot of disparity in the way the threats are handled and resolved. Many a times the government will have to step in during investigation and in case of subsequent arrests and detentions -- this is where cross border dialogue and diplomatic relationships will be important. Unfortunately, we don't see that many arrests yet when it comes to cyber crime as they are very carefully hidden in the big, bad World Wide Web.

A broader awareness level should be the priority. This has to be on an individual level, on a small and medium business level, and also at the large enterprise level. One of the statistics quoted in the report that was released in February 2015 by the Online Trust Alliance states that 90 percent of the breaches could have been avoided with basic cyber security practices. This implies that we need better encryption, stronger passwords, data protection during transit and at rest, modern security solutions, multi-factor authentication, data loss prevention technology among others best practices.[61] These are the basic best practices that should be applied from individual to an enterprise level. However, they are not being implemented, resulting in increasing data breaches.

The government should also take this up on its agenda and bring in the awareness. It can also re-look the policies that are put in place and amend them on basis of sector or business vertical. For instance, identifying the critical infrastructure for financial sector or energy sector and finding the information that needs to be prioritized and protected. These are the tangible steps that the government can take.

Looking at the broader perspective, global cooperation to put an end to cyber crime has improved significantly in the last few years, but it needs to go a lot further.

The above threat scenario raises the question of cyber security's direct impact on national, economic and human security and reinforces the urgency of capacity building in this field. India needs to quickly build its capacity across full spectrum of cyber security and ensure safe navigation through cyberspace for its prosperity and national security. Ensuring complete cyber security of our assets and National Information Infrastructure is thus both a national strategic imperative and an urgent national mission.

[61] ***Symantec's annual Internet Security Threat Report, 2015***

In pursuance of this objective, the Government of India released the National Cyber Security Policy[62] in July 2013 with the declared Vision," To build a secure and resilient cyberspace for citizens, businesses and Government" and Mission," To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation".

It is a very comprehensive document which was formulated over a period of two years and extensive deliberations with the Government, Industry, Academia and R&D organisations. Inputs were also taken from NASSCOM-DSCI document," Securing Our Cyber Frontiers "and IDSA Task Force report on cyber security. It not only lays down the objectives but includes the corresponding strategies for implementation. The Objectives spelt out are:-

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems 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 for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
- To enhance and create National and Sectoral level 24 x 7 mechanisms 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 enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

[62] *National Cyber Security Policy – 2013.*

- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.
- To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
- To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
- To provide fiscal benefits to businesses for adoption of standard security practices and processes.
- To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.
- To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
- To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Towards the end, the policy recommends to adopt a Prioritized approach for implementation so as to address the most critical areas in the first instance. It also suggests that this policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry,

department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace. It also emphasizes the absolute necessity of Public-Private Partnership and International co-operation.

Surprisingly, the Policy is silent on the capacity building for cyber warfare and development of cyber offensive capabilities. The then NSA, Mr Menon, however, when talking about Cyber Security Architecture mentioned that It will also involve capacity and authority for operations in cyberspace. It is presumed that this would be taken on by the NTRO, DRDO and Headquarters Integrated Defence Staff of the Ministry of Defence.

Cyber security is all about single point authority, responsibility and accountability; information sharing; concerted and co-ordinated efforts both at the National and International levels. It demands total synergy between various Ministries, Departments of the Central and State governments, Industry, R&D establishments and the Academia. This, unfortunately is lacking in the present dispensation. A few of the present major stake holder agencies for cyber security in India and at the global levels are listed in the succeeding paragraphs.[63]

National Information Board (NIB)

National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country.

National Crisis Management Committee (NCMC)

The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber-attacks.

National Security Council Secretariat (NSCS)

National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB.

[63]. ***Cyber Security and Related Issues: Comprehensive Coverage.*** *Y INSIGHTS · November 25, 2014 .*

Department of Information Technology (DIT)

DIT is under the Ministry of Communications and Information Technology, Government of India. DIT strives to make India a global leading player in Information Technology and at the same time take the benefits of Information Technology to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion & policies in electronics & IT.

Department of Telecommunications (DoT)

Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.

National Cyber Response Centre – Indian Computer Emergency Response Team (CERT-In)

CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. It maintains 24×7 operations centre and has working relations/collaborations and contacts with CERTs, all over the world; and Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country.

National Information Infrastructure Protection Centre (NIIPC)

NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence.

National Disaster Management of Authority (NDMA)

The National Disaster Management Authority (NDMA) is the Apex Body for Disaster Management in India and is responsible for creation of an enabling environment for institutional mechanisms at the State and District levels.

Standardization, Testing and Quality Certification (STQC) Directorate

STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. It has also established a test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.

The Cyber Regulations Appellate Tribunal

The Cyber Regulations Appellate Tribunal has power to entertain the cases of any person aggrieved by the Order made by the Controller of Certifying Authority or the Adjudicating Officer. It has been established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.The body is quasi-judicial in nature.

Inter-governmental organisations and initiatives
Council of Europe

The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Budapest Convention on Cybercrime, the Cybercrime Convention Committee (T-CY) and the technical co-operation Programme on Cybercrime. The Budapest Convention on Cybercrime was adopted on 8 November 2001 as the first international treaty addressing crimes committed using or against network and information systems (computers). It entered into force on 1 July 2004.

Internet Governance Forum (IGF)

The IGF was established by the **World Summit on the Information Society** in 2006 to bring people together from various stakeholder groups in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy making power in both the public and private sectors. The IGF facilitates a common understanding of how to maximise Internet opportunities and address risks and challenges. It is convened under the

auspices of the Secretary-General of the United Nations. Its mandate includes the discussion of public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

United Nations (UN)

The International Telecommunication Union (ITU) is the specialized agency of the United Nations which is responsible for Information and Communication Technologies. ITU deals also with adopting international standards to ensure seamless global communications and interoperability for next generation networks; building confidence and security in the use of ICTs; emergency communications to develop early warning systems and to provide access to communications during and after disasters, etc.

Conferences on Cyberspace

The London Conference on Cyberspace (1-2 November 2011) was meant to build on the debate on developing norms of behavior in cyberspace, as a follow-up to the speech given by UK Foreign Minister Hague at the Munich Security Conference in February 2011 which set out a number of "principles" that should underpin acceptable behavior on cyberspace.

Meridian Process

The Meridian process aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on Critical Information Infrastructure Protection (CIIP). Participation is open to all countries and targets senior level policymakers. An annual conference and interim activities are held each year to help build trust and establish international relations within the membership to facilitate sharing of information related to possible threats.

NETmundial Conference

In reaction to spying and surveillance activity by National Security Agency of USA through **PRISM**, NETmundial – Global Multi-stakeholder Meeting on the Future of Internet Governance(23 April 2014 – 24 April 2014) was organized in a partnership between the Brazilian Internet Steering Committee and /1Net, a forum that gathers international entities of the various stakeholders involved with Internet governance. This meeting focused on the elaboration of principles of Internet

governance and the proposal for a roadmap for future development of this ecosystem.

Cyber Security Current Status: India

The last decade has witnessed a slow but steady realisation within the Indian government and the Industry that the threats of the future will come from cyberspace. Unfortunately, while the realisation exists, the Indian security establishment has not been jolted into action in the manner in which the Kargil war or the 26/11 terrorist attack on Mumbai galvanised the nation to adopt a series of corrective measures. India was one of the first few nations to promulgate the IT Act 2000 which detailed a legal framework against cyber crimes. It is creditable that India could foresee the threat to her critical information infrastructure and introduced appropriate Sections 70A and 70B in the year 2008 while amending the Information Technology Act 2000.

It is sad that such a landmark and proactive legal provision went largely unnoticed in policy circles.

While announcement of the National Cyber Security Policy was a very welcome step, its implementation has been rather slow. Recently, the Government has given a fillip to capacity building in cyber security by bringing on line major projects and appointing a National Cyber Security Coordinator under the PMO.

Now, India is setting up its own **'Cyber Security Architecture'**[64] that will comprise

- the National Cyber Coordination Centre (NCCC) for threat assessment and information sharing among stakeholders,
- the Cyber Operation Centre that will be jointly run by the NTRO and the armed forces for threat management and mitigation for identified critical sectors and defence, and the
- National Critical Information Infrastructure Protection Centre (NCIIPC) under the NTRO for providing cover to 'critical information infrastructure'.

Concurrently, the government is also coming up with a legal framework to deal with cyber security; has launched a drive for creating greater awareness to this threat

[64] *India creating architecture to ensure cyber security: NSA*
indias*trategic.in/topstories1546_****India****_creating_****architecture****_to_ensure_*

and is creating necessary human resource with requisite skills. Major Cyber security projects under implementation are given in the succeeding paragraphs.[65]

National Cyber Coordination Centre (NCCC)

The government has approved the setting up a National Cyber Coordination Centre at an outlay of Rs. 770 crores. NCCC is a critical component of India's cyber security against hackers and espionage as well as track terrorist activity on line. It is likely to start operations by the end of year 2016. A group of cyber security professionals and experts will look after the functioning of the Centre and track illegal and terror activities on line. It will run on similar lines as in the US, UK, France and Germany.

Setting up of NCCC is the responsibility of Computer Emergency Response Team-India (CERT-In). It will function under the National Information Board. Some of the components of NCCC include a cyber crime prevention strategy, cyber crime investigation training, review of outdated laws, etc. It is expected to coordinate between intelligence agencies specifically during network intrusions and cyber attacks. Its mandate may also include cyber intelligence sharing. Indian and U.S. intelligence agencies are also working together to curb misuse of social media platforms in the virtual world by terror groups.

Botnet Cleaning and Malware Analysis Centre

To obviate and limit the threat due to botnets**,** the Government is setting up a Botnet Cleaning and Malware Analysis Centre at an envisaged investment of Rs. 90.5 crores. The project is being implemented on fast track and is likely to be available in the next three months. It is a part of Digital India programme and aims to create safe and secure cyberspace. It will automatically detect botnets that trigger various cybercrimes and suggest the device owner to remove them from their device with their help.

Central Monitoring System (CMS),

Central Monitoring System, the Union Government's ambitious electronic intelligence monitoring system, is likely to start functioning by this year-end. According to the Ministry of Home Affairs officials, the hi-tech unit which will provide unhindered access to phone calls, text messages, and social media

[65] *CHALLENGES AND PROSPECTS OF CYBER SECURITY IN INDIAN CONTEXT (USI: 20 May, 2015) By Lt Gen Davinder Kumar*

conversations to law enforcement agencies in real-time will have two units in the inaugural phase in Delhi and Bangalore.

CMS was conceptualised by the Department of Telecom after former National Security Adviser Shiv Shankar Menon decided to put in place a robust system for monitoring calls. It aims to stop the leakage of information from the service providers' end by building a centralised monitoring system, which will be monitored by the agencies, authorised to intercept the calls and internet communication. As per the government's strict norms for interception of calls, violation by any private agency or individual can result in a jail term of five years and fine of one crore rupees.

The total cost of the project would be approximately 590 crore rupees. Entire monitoring system which is being designed and integrated by the Telecom Enforcement, Resource and Monitoring (TERM) and C-DoT will be supervised by the Intelligence Bureau. All the interception platforms, including PSTN, GSM and CDMA technology, will be easily intercepted as CMS would provide convergence of all lines at one location.

National Critical Information Infrastructure Protection Centre (NCIIPC)

Article 70A (2008) mandated the need for a special agency that would look at designated CIIs and evolve practices, policies and procedures to protect them from a cyber attack. But the then United Progressive Alliance government took another six years to create such an agency. On January 16, 2014, the Department of Information Technology (DIT) issued a notification announcing the creation of a specialised body to protect India's CIIs. The National Critical Information Infrastructure Protection Centre (NCIIPC) was created and placed under the technical intelligence agency, the National Technical Research Organisation, to roll out counter-measures in cooperation with other security agencies and private corporate entities that man these critical sectors.

A "critical sector" has been defined under the notification as "sectors that are critical to the nation and whose incapacitation or destruction will have debilitating impact on national security, economy, public health or safety".

The government has identified 12 sectors that fit the bill and can be covered under the NCIIPC project as mandated by Section 70A of the amended IT Act. These range

from energy to power, law enforcement, aviation, banking, critical manufacturing, defence and space. While several of them are housed within the government, sectors such as energy and power are manned by the private sector. Hence protection of CII is a joint responsibility of both the Public and Private sectors and it demands both synergy and mutual trust. They must jointly develop appropriate plans, adopt requisite standards, share best practices, and refine procurement processes in respect of protection of Critical Information Infrastructure. This will mean sitting together to conduct joint exercises, map vulnerabilities, build counter-measures and achieve a synergy that it is currently lacking.

Protection of Power Sector[66]

In December 2010, Ministry of Power had constituted CERTs (Computer Emergency Response Teams) for power sector i.e :-

- CERT-Thermal (nodal agency- National Thermal Power Corporation (NTPC),
- CERT-Hydro (nodal agency- National Hydroelectric Power Corporation (NHPC)) and
- CERT-Transmission (nodal agency- Power Grid Corporation of India Limited (PGCIL)

to take necessary action to prevent cyber attacks in their domains. The State Power Utilities have also been advised to prepare their own sectorial Crisis Management Plan (CMP) and align themselves with the Nodal Agencies i.e. NTPC, NHPC & PGCIL and CERT-In for the necessary actions**.**

Grid Security Expert System (GSES)

Grid Security Expert System (GSES) was proposed to be developed in March 2015, by POWERGRID and it involves installation of knowledge based Supervisory Control and Data Acquisition (SCADA) system, numerical relays and Remote Terminal units up to 132 kV stations and the reliable Optical fibre Ground wire (OPGW) communication system at an estimated cost of around Rupees 1200 crores. The objective of the GSES is implementation of the Automatic Defense mechanism to facilitate reliable and secure grid operation.

[66] *National power grids hit by cyber terrorist onslaught.07/04/2015*
http://www.itproportal.com/2015/04/07/cyber-terrorists-target-national-power-grids/#ixzz45niOuKZ3

Besides, CERT-In (Computer Emergency Response Team-India), Department of Information Technology, Ministry of Communication and Information Technology, Government of India has prepared a Crisis Management Plan (CMP) for countering cyber attacks and cyber terrorism for preventing the large scale disruption in the functioning of critical information systems of Government, public and private sector resources and services. The Crisis Management Plan (CMP) for Countering Cyber Attacks and Cyber Terrorism outlines a framework for dealing with cyber related incidents for rapid identification, swift response and remedial actions to mitigate and recover from cyber related incidents impacting critical national processes.

Network Traffic Analysis System (NeTRA)

A monitoring and electronic surveillance project being executed by the DRDO**.** It will intercept and examine communication over the internet for keywords like 'attack', 'blast', 'kill'. It appears to be Indian government's first attempt of mass surveillance rather than individual targets. It will scan the activities over the social networking websites like twitter and would scan the mails and chat transcript and even the voices in the internet traffic.

Challenges

It would be seen that these efforts are aligned towards developing a cyber defence capability. There is no information in the open domain regarding development of cyber offensive capabilities and their integration. Cyber space is essentially "Offence Dominant" by its very character and cyber power includes both defensive and offensive capabilities. India needs to develop full spectrum cyber capabilities without any further delay particularly in light of major national projects like Digital India. National Broad Band Network, 100 smart cities, Make in India and the emergence of China as a cyber super power.

This needs national scale effort supported through political will, a dedicated and empowered organization; assured funding, contemporary technology, an electronic manufacturing eco system, focused R&D and skilled people to realize necessary cyber security capability. Each of this presents a unique challenge and demands total synergy amongst various ministries and agencies through appropriate policy framework and must be addressed concurrently. Some of the main challenges are given in the succeeding paragraphs.

Organisation

India needs to Establish "National Cyber Security Commission" (NCSC)[67] – a fully empowered body with its own department, on the lines of Space Commission and Atomic Energy Commission. The country needs to build thought leadership and weave together India's potential in cyber security under one organization. National Cyber Security Commission must be headed by a technocrat with the position of a Cabinet Minister. All central agencies like NCIIPC, CMS, and NCCC should be placed under this organization. The states must have a separate and dedicated set up for cyber security on the lines of disaster management, fully integrated with the NCSC; their CERTs linked up with the CERT-In with emphases on information sharing and incident reporting.

Review the National Cyber Security Policy 2013 to include development of full spectrum capabilities; a policy frame work to ensure total synergy amongst various organs of the Government, industry, R&D establishments and academia; organization; technology, R&D, standards, testing facilities and a vibrant electronic industrial base; availability of necessary skilled resource, their constant training and retention; assured budgetary support, international cooperation and a legal frame work. This policy should be translated to a time bound action plan, a national cyber doctrine and specify clearly the responsibility for its execution and accountability. The policy, action plan, organisation and assured budgetary support must be discussed and approved by the Parliament.

Develop Cyber War Capability: India urgently needs to develop policies and capabilities in this 'Fifth' domain of war. These cannot wait and must be taken up on top most priority in a "Mission Mode" by the Services. The situation and threats to India are unique and hence there is the necessity of developing an Indigenous solution in consonance with the Doctrine to include Organisation, Technology, Skill sets and R&D in a very tightly monitored time schedule.

Within the overall structure, a time bound action is needed for raising of a dedicated "Defence Cyber Agency". Call it by any name, so long it has the capability across full spectrum of cyber/information operations and the necessary muscles to protect, bite and ensure freedom of action in Cyberspace and deny the same to our Adversaries'.

[67] *VIF Report on Cyber Security*

National Electronic Policy (NEP) 2012[68]

India imports upto 90 percent of electronic goods and components. This places her at total security risk through cyber interventions of our networks and systems. The malware can be injected either through the supply chain or through installation of trojans and logic bombs during manufacturing which are directly under the control of the supplier and can be released at will. NEP 2012 was promulgated to neutralize this strategic vulnerability in our national security and accordingly had laid down the policy to establish an Electronic System Design and Manufacturing (ESDM) eco system in the country. It also had the proposal of establishing FABs for making semi-conductor chips in the country. Unfortunately, the scheme did not take off inspite of the fact that it offered attractive financial and taxation terms. This scheme has now been given a push under the "make in India" programme. Establishment of ESDM and FABs are absolutely essential and fundamental pre-requisites for cyber security and need immediate attention at the highest level.

Cyber Workforce Development:

When one talks about readiness in India, one of the big challenges is in terms of talent availability. The initial Cyber Security Policy 2013 had identified a requirement of half a million cybersecurity professional. A February 2014 report of the parliamentary standing committee on IT found that at that time there were less than 75,000 people who were ready. This is a huge gap that presents both a great challenge and a huge opportunity for India to scale up not just to protect information and assets in the country but also globally. This requires a strong public-private partnership and out of the box measures. For example, a fair estimate indicates that the NCC (National Cadet Corps) could provide up to 125,000 cyber personnel in three years' time frame. We not only need to develop a separate cyber security cadre but also cyber leaders and trainers.[69] We also must lay emphasis on developing Science of Cyber Security.

R&D for Product Development:

There is no focused R&D with a well thought out plan to develop cyber security technology, products, e-mail and social media platforms, with sponsored projects in the private sector. Funding in universities with no accountability for outcomes has

[68] *National Policy on Electronics – 2012*

[69] *A Cyber wing in the NCC- by Lt Gen Davinder Kumar*

not led to any innovation in any dimension of cyberspace. We need focused R&D in the development of safe products, discovery and analysis of vulnerabilities, fixing attribution and design of cyber weapons and skills for converting "engineering in to production".

Security Standards and Frameworks, Audit: India needs to develop and promulgate the cyber security standards and frameworks for development, and audit processes for assurance of protection of our NCII. Enabling Policy measures are required to encourage establishment of testing labs for managing ICT Supply Chain Risks, developments of safe products and execution of secure projects.

Cyber-crime investigations: There is an urgent need for development and continual upgradation of Cyber forensics capabilities and investigating skills with our law enforcement agencies (LEAs), to handle cyber crimes in the ever expanding proliferation of devices, platforms, big data, Internet of Things, mobility and social media.

Assurance Framework, Test & Certification: There is an immediate requirement of setting up a national cyber test facility providing for network emulation, monitoring and audit, vulnerability analysis, simulated attacks, graduated response, performance analysis and security assurance modeling in next 12 to 18 months.

Development of Indigenous Software and Network Products: There is a fundamental requirement of developing indigenous software like an Indian Operating system, Search engine, encryption and social media like Facebook and twitter. We also need to design and produce Indigenous net work and security products.

Build Thought Leadership, Executive/ Political Sponsors: Build cyber security savvy leadership, subject matter experts, solution architects and system engineers so as to address the inadequate comprehension of lack of cyber security capability and its bearing on national security including the military dimension. Foster system thinking - strategic, ahead of times, at national scale about cyber warfare as replacement/ co- existing with components of Kinetic Energy Weapons (KEWs) in the country in step with the rest of the world. Build operational requirements, articulate and validate cyber doctrine as standalone option or in tandem with KEWs in training exercises and war games.

Conclusion

Cyber security is a major concern of the 21st century. The situation is going to become worse with the galloping pace and increasing penetration of ICT and equally the anti-technology to neutralize the same. The large scale fielding of IoT, virtual currency, Cyber weapons, dark web and so on will present new challenges and the threat landscape is going to become quite scary and will require almost real time management. Cyber security will always remain a "work in progress".

Never before in the history of mankind, has the individual security and privacy been so challenged. One would think that cyber security would be dealt with at the same level as terrorism and climate change by the next decade. The threat and hence the challenge is huge and requires global approach and international efforts.

India needs to expedite capacity building in cyber security across full spectrum and implement measures to ensure her economic development, national and individual security through assured and unhindered passage in cyber space This is a strategic imperative and India cannot afford to delay or neglect it.

Image Source:

- http://drishtikone.com

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media fields have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organization to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelize fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its establishment, VIF has successfully embarked on quality research and scholarship in an effort to highlight issues in governance and strengthen national security. This is being actualized through numerous activities like seminars, round tables, interactive-dialogues, Vimarsh (public discourse), conferences and briefings. The publications of the VIF form the lasting deliverables of the organisation's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org, Website: http://www.vifindia.org
Follow us on twitter@vifindia