International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, September 2015
www.ijates.com
ijates
ISSN 2348 - 7550

CYBER INTELLIGENCE SHARING AND INTERNATIONAL COOPERATION

Gp Capt Devesh Vatsa[1], Maj Gen (Dr) GS Lamba VSM (Retd)[2], Dr. K P Yadav[3], Wg Cdr Vikas Sood[4]

[1,4]Research Scholar, Dep of IT, Noida International University, (India)

[2]Principal, Baba Banda Singh Bahudar Engg College, (India)

[3]Dir KCC Institute of Tech & Management, (India)

ABSTRACT

The extensive ingress of Information & Communication Technology (ICT) has transformed the way businesses and Governments operate worldwide. Cyber Space is becoming lucrative target for hackers as it is getting richer and richer due to continuous migration of processes, procedures, functions & operations including that of critical systems. Cyber threats, being a low-cost asymmetric warfare element, pose a direct threat to the security of the nations'critical infrastructures . The risks of operating in cyber world are reaching unprecented levels as newer forms of threats and vulnerabilities continue to emerge. Such threats are becoming harder to predict as well as targeted in nature. With the ever-shrinking difference between the cyber and physical world, and the use of a large number of internet-connectd devices, the threat actors are seemingly well positioned to cause disruption to a nation's government, business and citizens alike. Non-state actors like IS and Al-Qaeda, who have extensively used ICT to achieve their objectives, are the most suitable example apart from many state actors involved in cyber espionage & cyber attacks. As technology continues to offer numerous benefits to society, a number of divergent scenarios continue to stifle its widespread adoption and growth. In order to prevent such misuse of ICT for criminal activities, a higly coordinated effort is required between country's government, businesses, citizens as well as collaboration with international agencies. In the world of complex Cyber Space, no individual organisation will be able to defend them without the collective sharing of threat and attacker intelligence. Therefore, different countries, private sector and public sector need to co-operate & collaborate in developing the strategies to minimise the impact of Cyber Attacks on Information Infrastructure both critical & non-critical. This paper examines the need of cyber threat intelligence sharing; methodology involved; and challenges & issues involved in sharing intelligence. The paper also highlights the existing organisations for cooperation and recommends an approach towards cyber intelligence sharing at National & International level.

Keywords: Collective Defence, Cyber Threat, Cooperation, Cyber Criminals, Cyber Defence, Security, Cyber Terrorism, Cyber Deterrence

I. INTRODUCTION

The huge penetration of Internet in the life of people world over (40% of world population i.e ~ 3.19 billion) has changed the medium of correspondence to the cyberspace. Millions of people, devices and machines are getting hyper-connected across the world every day. Enormous amount of real-time information is moving across the ever expanding network at increasing speeds. The Cyber Space is being utilised by businesses to enhance efficiency & enable them to compete effectively in the global economy whereas the governments worldwide are using the platform for improved governance. All types of services like banking, health services, transportation, marketing & sales, entertainment, hospitality etc. are being extended to citizens through Cyber Space. This is validated by the various activities being undertaken electronically like e-commerce, e-auction, e-procurement, e-education, e-filing of tax return, e-governance, e-banking, e-health etc. The mammoth migration of physical data to virtual data has made the cyberspace extremely rich and the process of migration is still on. Such powerful capability also comes with significant vulnerabilities. The very capability that can enable e-banking, telemedicine, e-auction, e-commerce, e-governance in seconds can disrupt life if misused by the malicious actors. The Cyberspace being extremely rich is always a lucrative target for a variety of cyber criminals including state and non-state actors due to inherent lack of security by design. The over dependence of people on the Global Common called Internet for all kind of services all over the world has provided an opportunity to the Cyber Criminals to exploit the existing vulnerabilities in the ICT which runs the Internet. These vulnerabilities are exploited by Cyber Criminals to launch cyber-attacks to achieve their objective which can vary from financial gain to jeopardising the national security of the country. The information breached includes corporate secrets & intellectual property, highly secret documents & records of Government, Personally Identifiable Information & Health Information of individuals, Financial Information of banks & Credit card industry and extremely Private Information of individual. The basic aim of the Cyber Criminals is to steal sensitive and secret information which can be sold for a price. Protection of country's assets from Cyber Attacks is a big challenge and needs unprecedented collective action. Collaboration improves everyone's cybersecurity preparedness.

The rapid growth of online social networking applications has resulted in its use both for personal and professional work. In present age, social media has become an integral part of the lives of people, providing them a platform to communicate, share, connect, opine and curate with family, friends, social groups and other community. The emergence and unstoppable growth of social networking sites such as facebook, twitter, viber, skype, wiki, you tube are clear indicative of their extensive usage satisfying varied needs of users. Social media has revolutionised the world like newspaper, radio and television did in the past. It has helped in forming the public opinion about the brand, government, political parties, and individuals apart from keeping them abreast of the happenings around the world. However, the basic difference between the media of past and social media of current times is that the social media is instantaneous & interactive compared to the media of past which was primarily simplex or one side communication. Rebuttal to any news or views in the newspaper, radio or television could not be immediate but in case of social media it is immediate. However, the social media has become a very powerful tool for hacking into the computer systems and becomes highly potent when coupled with social engineering. Social engineering is a technique to steal identity credentials of people by fooling them by various means.

Cyber Attacks could have a potentially devastating impact on the nation's computer systems and networks, disrupting the operations of government & businesses on one hand and the lives of private individuals on the other. Increasingly sophisticated Cyber Threats have underscored the need to manage and bolster the Cyber Security of key government systems as well as the nation's Critical Information Infrastructure (CII). With greater dependence on networked systems and reliance on the integrated networking today, our defence systems are faced with ever increasing threat and thereby securing them is a great challenge. The recent breaches in the various Information Infrastructure worldwide from operations like Stuxnet, Red October, APT1, Flame and very recently Sony hack have forced the Industry as well as Defence to have a relook at Cyber Security aspects associated with protection of their Information Infrastructure. The day is not far when our Supervisory Control And Data Acquisition (SCADA) systems and Industrial Control (IC) systems which are presently working in silos & insulated environment will migrate to Internet and expose themselves to cyber-attacks. The problem will only become much grave with adoption of Internet of Things (IoT) and Smart Cities.

To overcome the challenges posed by ever increasing cyber threats, the government, businesses and academia have to collectively work and collaborate to evolve strategies to mitigate the risks from cyber-attacks. Cyber intelligence sharing is one such strategy which can enhance our capabilities and situational awareness towards handling the menace of ever increasing cyber-attacks. Cyber threat intelligence sharing will enhance the knowledge of all stakeholders about cyber-attacks, malware, modus operandi, indicators, vulnerabilities, timing etc.

II. CYBER TERRORISM

Cyber terrorism has been defined as "a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda". Ultimately cyber terrorism can surely be seen as being related to both hacktivists and patriotic hackers, differing largely in both the scale and the intensity of their actions. The term cyber terrorism may be mixed up with information warfare" and "cybercrime". But there is a major difference between cyber terrorism and information warfare. Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets. But older term known as information warfare is defined as "a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses."

Information warfare also encloses the term "cyber warfare". But cyber warfare's interest is limited to cyberspace. Information warfare and cyber warfare have "certain targets" in a war but cyber terrorism causes fear and harm to anyone in the targeted vicinity.

III. INTERDEPENDENT SECURITY

In present scenario, the security is interdependent as cyber space by nature being international has no traditional boundaries and we depend on other countries for crucial inputs. This demands that we acknowledge security

levels of other countries and try to align or adopt the best practices being followed by them. It is in our own best interests to share the following:

- Reports of threat analysis; approach adopted to mitigate risk.
- Steps taken for security capability enhancements (Prepare, Detect, Respond, Recover capabilities).
- Best Practices against malware to combat cyber crime.
- Network contacts with Subject Matter Experts.
- Participate in Trans-Border Experiments / Exercises.

IV. CONCEPT OF COLLECTIVE DEFENCE

It is well known that the cyber world transcends all physical barriers. Being transnational in nature, it is but obvious that nations across the globe need to strengthen their cooperation and form alliances as well as ensure that their legal, technical and institutional measures; structures are created; and work in coherence. Collective defence requires a deeper cooperation among partners that goes beyond cyberspace itself. There is a requirement for international strategy for cyber space that requires formal and informal engagement efforts to improve cyber security, and that ultimately promotes collective national security, stability, and deterrence. Forward-looking national cyber security initiatives are vital to the stability of the global digital economy. Collectively we need to:

- Examine cyber-capability requirements to prepare for, protect from, and respond to cyber-attacks and their potential effects and impact.
- Exercise strategic decision-making and inter-agency coordination for incident response(s) in accordance with strategic and national-level security policies, procedures, and reactions.
- Conduct research into how we authenticate information and communications sharing relationships and the impact of increased public-private collaboration and cooperation.
- Examine the frameworks for collecting and disseminating cyber incident situational awareness, response, and recovery information.
- Examine and validate the means, processes, and policies related to the sharing of sensitive information across boundaries and sectors, without compromising collective national security interests.

Therefore, to achieve all of the above, it is necessary that nations are able to reach consensus and work toward establishing a framework of international cooperation.

V. ATTACKERS ARE GETTING INCREASINGLY SOPHISTICATED

There is always a technological gap between security agencies and the attackers. This is called as the “security gap”. It is evident from use of zero-day exploits by the hackers that there are a number of vulnerabilities in the systems which are being exploited in the grey market and they come to open only in case of a breach of security or on hacking of hackers. Today, attackers are getting sophisticated and following have been observed:

- Coordinated attacks are launched from hacker communities spread across geographies.
- Driven by personal, financial, societal agenda.
- Sophisticated strategies are used to avoid detection.
- Targeting systems that users trust to camouflage malicious code / malware.

- Exploiting vulnerabilities within unpatched systems and weak applications.
- Exploiting vulnerable users through targeted spam campaigns.
- High understanding of business applications and their logical workflows.
- Focus on critical infrastructure – SCADA & new technologies -- IoT

Fig-1 Depicts a typical screen shot of the cyber threat real time map based on Kaspersky Lab inputs. As it is visible the number of attacks are increasing exponentially amongst various countries.

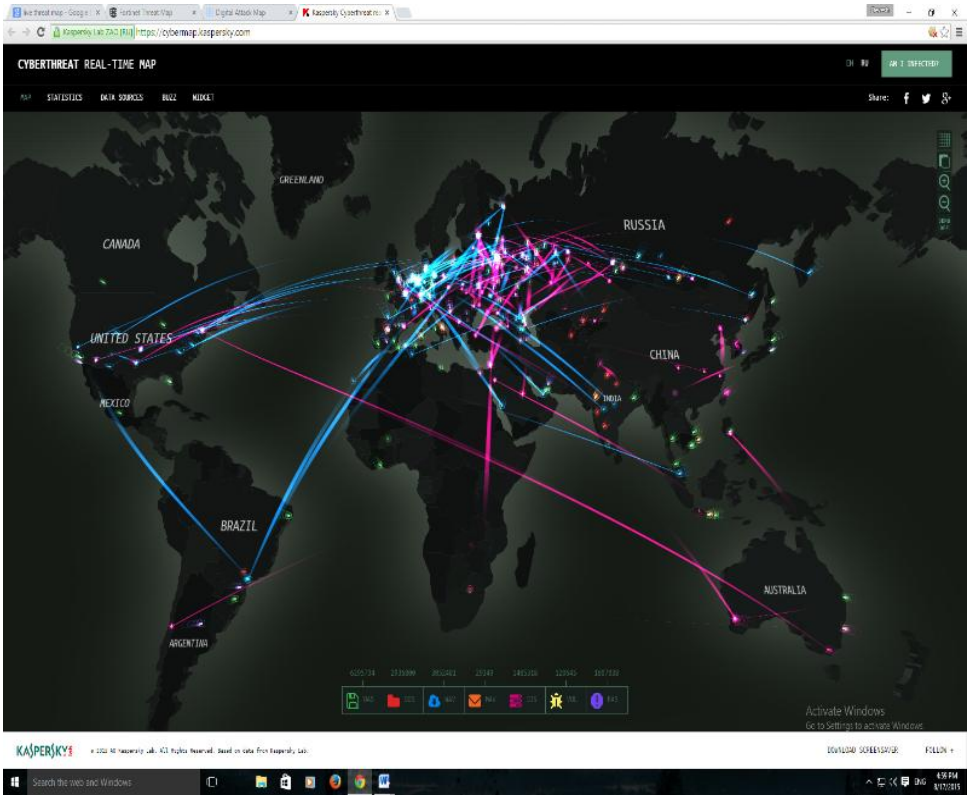

Fig-1 Cyber Threat Real Time Map (Source Kaspersky Lab-2015)

VI. CAUSE OF CONCERN

The breaches in past indicates that there has been a massive drive to steal the sensitive data for financial and strategic gains by various actors. The following breaches bring out the details of losses to the organisation and number of consumers whose data has been stolen.

- **The Global Cost of Cybercrime**: More than $400 Billion per Year - McAfee Report on Global Cost of Cyber Crime.
- **Ponemon Institute's 2014** Cost of Cyber Crime study finds cyber-attacks cost the average U.S. Company $12.7 million with some surveyed companies experiencing losses up to $61 million.
- **Cybercrimes** have cost India a whopping about Rs 24,630 crore (US $ 4 billion) in 2013 alone as criminals used sophisticated means, says a Delhi High Court-commissioned report.
- **Hackers** stole personal information of about at least 22.1 million people, including addresses, mental health and criminal records, in two major breaches of U.S. government databases.

- **US Department of Commerce** report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually.
- **The Organisation for Economic Development (OECD)** estimated that counterfeiting and piracy costs companies as much as $638 billion per year.
- **2007:** TJX's credit/debit card hack cost about $250 million, 94 million customers affected.
- **2013:** Target reported the price tag for its credit/debit card breach would reach $148 million, 40 million customers affected.
- **2014 :** Home Depot acknowledged that it has to pay at least $62 million to clean up the breach, 56 million credit-card accounts & 53 million customer email addresses were stolen .
- **2014:** Sony Pegs Initial Cyber-Attack Losses at $35 Million.
- **Feb 2015**: 80 million customers of health insurance company, Anthem Inc., have had their account information stolen. It included names, birthdays, medical IDs, Social Security numbers, street addresses, e-mail addresses and employment information, including income data.
- **March 2015**: 11 million customers and employees of a major health insurer, Premera Blue Cross, have had their sensitive info exposed.
- **July 2015**: UCLA Health System data breach affected 4.5 million people. It included names, Social Security numbers, medical records, ID numbers and addresses.

VI. CHALLENGES OF SECURITY IN CYBERSPACE

The protection of cyberspace from ever evolving cyber threats is a big challenge for professionals responsible for information assurance, security and governance. The characteristic of cyberspace makes it not only vulnerable but very difficult to protect it from cyber threats. The primary reason for cyberspace for being under constant cyber attacks is its inherent nature of being boundary less and extremely rich with all types of data including secret, sensitive and personal data. Attacking the cyberspace is very easy as proximity to target is not essential due to the ubiquitous nature and highly pervasive internet providing access. Defending the cyber space is extremely difficult because of the inherent vulnerabilities in the hardware, software, firmware and applications which are major constituents of ICT devices which forms the cyberspace. The attribution is another challenge as identifying the attacker is a herculean task with little or no success. The actors involved in cyber attack, the challenges in attribution, the activities of actors and who could be responsible authority are elaborated below.

7.1 Actors

- A key challenge of cyberspace is that it is populated by both state and non-state actors.
- These two categories of users are not readily identifiable. It is for the sovereign states to ensure that non-state actors within their jurisdiction respect the law, including international legal obligations that have been incorporated into national law.
- The cyber criminals or terrorists residing in a country A and targeting victims in another country B while insulated from direct action of law enforcement agencies of country B are still the responsibility of the country A in terms of any collaborative treaties signed between the two countries.

- To achieve effective implementation very close, proactive and flexible interaction between law enforcement agencies of the two signatories is essential. The matrix becomes more involved when the number of member states increases and the ecosystem should evolve to bring in transparency amongst all stakeholders.

7.2 Attribution

- In cyberspace, a cyber-attacker can hide him readily, and even disguise his attack to appear to originate from a third party.
- The problem of attribution for a cyber-action is clearly one that will complicate any effort at security controls.
- Uncertainty about attribution will also constrain retaliatory action.
- The current level of research in reliable attribution is not adequate.
- The cybercrime treaties cannot be implemented unless trust exists between signatories that best efforts are being put to identify the criminals and therefore, transparency is first precondition for success.

7.3 Authority

- The designation of a state agency that would lead the response to an international cyber-attack would depend on the nature of the attack.
- The vast majority of hostile cyber-activity originates with criminal elements, for which law enforcement agencies are normally responsible.
- A response to use of the Internet by terrorists might entail pooling resources from both the national security and law enforcement communities.
- The fact that hostile international cyber-activity is not exclusively or even predominantly a national security phenomenon adds a further complication to the development of internationally acceptable approaches for regulating or policing such activity.
- International collaborative initiative for countering cyber- crime; the 2001 Budapest Convention on Cybercrime by the Council of Europe has run into road blocks in absence of mutual trust and attempts to erect barriers to the operational procedures (remote log in to the suspected computer systems)considered crucial for timely collection of the evidence, which is in any case very fragile.

7.4 Activity

- Hostile international cyber-activity, as already noted, can be perpetrated by state or non-state actors. Within state actors too, the military and intelligence arms of nation states operate under different norms.
- Intelligence agencies of all countries with means and capacity will keep tabs on adversaries and on activities they perceive as threats. No international agreement or legislation will change that. When such attempts to spy are exposed, as by Snowden, there will be a degree of furor and then it will be business-as-usual

VIII. INITIATIVES AT INTERNATIONAL LEVEL

Towards mitigating the risks emanating from ever evolving cyber threats many countries have opted for mutual cooperation for resolving cyber related issues and formed various bi-lateral and multi-lateral organisations. The important ones are listed below.

- United Nations General Assembly
- International Telecommunication Union (ITU)
- Interpol / Europol
- The Organisation for Economic Cooperation and Development (OECD)
- UN Organisations on Drug and Crime Problems (UNODC)
- UN Interregional Crime and Justice Research Institute (UNICRI)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- International Organisation for Standardisation (ISO)
- The International Electro technical Commission (IEC)
- Internet Engineering Task Force (IETF)
- Forum of Incident Response and Security Teams (FIRST)

The various organisations kept on forming from time to time to mitigate the risks emanating from ever evolving cyber threats. Few of them along with their objectives are mentioned below.

8.1 2001 Budapest Convention The first international treaty seeking to address Internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.

8.2 2001 The Council of Europe It adopted a Convention on Cybercrime to improve international cooperation in combating actions directed against the confidentiality, integrity, and availability of computer systems, networks, and data. The council also sponsors training and conferences to address cyber security issues.

8.3 2004 The London Action Plan (LAP) Founded with the purpose of promoting international spam enforcement cooperation. Since inception, LAP has expanded its mandate to include additional online and mobile threats, including malware, SMS spam and Do-Not-Call.

8.4 2004 Digital PhishNet Developed jointly by the FBI's National Cyber-Forensics & Training Alliance, various law enforcement and industry stakeholders as a means to better collect and develop intelligence regarding the highest priority and most sophisticated phishing (identity theft) schemes.

8.5 2008 IMPACT The International Multilateral Partnership Against Cyber Threats (IMPACT) is a key partner of the International Telecommunication Union (ITU), a United Nations' (UN) specialised agency, in the effort to ensure the safety of cyberspace for everyone.

8.6 2009 CCDCOE Its mission is to enhance the capability, cooperation and information sharing among NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

8.7 2009 The National Security Council (NSC) It has approved an Information and Communications Infrastructure Interagency Policy Committee which subsequently approved a subcommittee to focus on global cyberspace policy efforts.

8.8 2009 GMU International Cyber Centre Facilitate strategic collaboration and information sharing to better identify, coordinate among stakeholders and address global cyber issues.

8.9 Interpol Collects, stores, analyses, and shares information related to cyber crime between its 188 member countries through its global police communications system. It is also responsible for coordinating operational resources such as computer forensic analysis in support of cyber crime investigations. Additionally, INTERPOL has a network of investigators in national computer crime units to help law enforcement seize digital evidence as quickly as possible and facilitate cooperation when a cyber attack involves multiple jurisdictions.

8.10 Asia-Pacific Economic Cooperation's Telecommunication and Information Working Group Supports security efforts associated with the information infrastructure of member countries through activities designed to strengthen effective incident response capabilities, develop information security guidelines, combat cyber crime, monitor security implications of emerging technologies, and foster international cooperation on cyber security.

8.11 U.S. Department of Homeland Security Is responsible for preventing and deterring terrorist attacks and protecting against and responding to other threats and hazards within the United States, including with regard to key resources and critical infrastructure. DHS is also tasked with critical infrastructure protection responsibilities that include strengthening international cyberspace security in conjunction with other federal agencies, international organisations and industry.

IX. ADVANTAGES OF SHARING CYBER INTELLIGENCE

The advantages which can be accrued through cyber intelligence sharing amongst various stakeholders are many both at national and international level. Few are listed below.

- Real-time sharing that can enable the widespread knowledge of the threat environment.
- Improved insight into cyber attack behaviour.
- Reduced time to mitigation of many threats as they appear.
- Cross-sector threat views providing a more robust and comprehensive understanding of threats that enable all sectors to more effectively defend their environment.
- Breach Avoidance.
- Analyst force multiplication by leveraging research and analysis being done in the industry.
- Decrease time to detection of malware and targeted attacks.
- Increase analyst efficiency.
- Reduced the man-hours spent acquiring and operationalising indicators.
- Accelerated incident response by reducing event analysis time.
- Detect lingering adversaries & historical attacks.

Apart from the advantages as brought out above the threat intelligence sharing will also help in answering the following questions:

- What was the attack ?
- When did it happen ?
- Where was it found ?
- What does the attack look like ?
- How is it affecting the environment ?
- What was the impact ?
- What was the surrounding context ?
- How quickly was it solved ?

X. ENTITIES UNVEILED BY INTELLIGENCE SHARING

- **Threat Actors** Sharing intelligence about nation-state activities, organised cyber criminals and hacktivists.
- **Vulnerabilities and Exploitation** Sharing intelligence on zero-days and CVEs on regular basis.
- **Mechanisms and Indicators** Sharing of results of malware analysis, knowledge of APTs, mobile malware & DDoS technology, monitored command and control infrastructures, etc.

The knowledge obtained through threat intelligence sharing can be converted into actionable advice providing partners with ongoing hacking activities; and drive decision advantage over the adversaries that confront them. The threat intelligence sharing not only enhances situational awareness but also helps in capacity building.

XI. CHALLENGES IN SHARING INTELLIGENCE

The major hurdles in sharing threat intelligence can be clubbed in three broad categories.

- **Legal** Sharing of cyber-information within the government's possession and sharing of cyber-information within the possession of the private sector.
- **Financial** Collecting threat signatures or other threat indicators, and then selling that information to other security providers is a revenue source for many companies.
- **Technical** All stakeholders realise that "active" cyber defence, based on real-time threat awareness and machine-to-machine sharing and mitigation, is the only strategy that will enable confidence in the environment in which government and business operations are conducted. A number of technical issues related to the definition and adoption of the standards & protocols needs to be addressed.

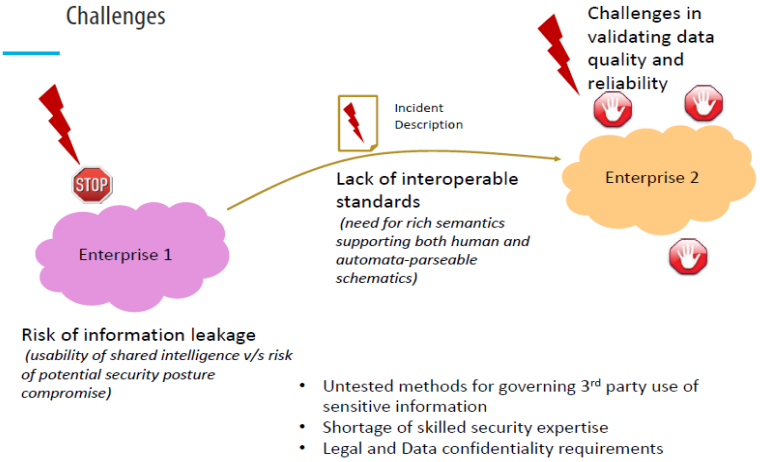

Fig-2 Challenges in Sharing Intelligence

The above figure depicts the snapshot of challenges involved in sharing intelligence. There are many challenges which need to be overcome for effective sharing of cyber intelligence. Significant challenges are listed below.

- Information is unreliable or out of date.
- Fear of inadvertently sharing sensitive company information.
- Potential security posture compromise.
- Trust deficit.
- Whom to contact to share.
- Lack of interoperable standards and lack of proper Taxonomy.
- Challenges in validating data quality and reliability.
- Attribution
- Differentiating Cyber terrorism & Cyber Deterrence
- System Integration
- Situational Awareness & Virtualisation.
- Supply Chain Security.

XII. PRIORITY AREAS IN COOPERATION AND COLLABORATION IN CYBERSPACE

12.1 Implementation of Dynamic Responses to Cyber Incidents In implementing the risk-based approach premised on the possibility of cyber incidents, response needs to be prompt and global, and must minimise the impact of the incident while addressing the ever-changing risks. As cyber threats are real threats, building a mechanism for international cooperation and partnership is an urgent task. Such mechanism would facilitate quick identification of a cyber-incident, accurate analysis of its impact, and global dynamic response to the incident such as prevention of further damage, facilitation of early resolution, research on its causes and prevention of similar incidents.

12.2 Enhancing multi-layered mechanism for information sharing In order to establish a mechanism which can dynamically respond to global cyber incidents, there also needs to be a mechanism for global information-sharing which enables responses based on international information and sharing of countermeasures. Having a wide range of information sources facilitates quick and accurate judgments on

the rapidly-changing situations, given that diverse entities are involved in cyberspace with their own security measures. Thus, it is meaningful to build an information-sharing mechanism that is multi-layered, consisting of multiple layers including technology, law enforcement, policy and diplomacy. In particular, it is important to develop cooperation among Computer Emergency Response Teams (CERTs), which are responsible for operational responses, such as detecting cyber incidents, analysing malwares and IP addresses and taking actual responses; cooperation among law enforcement agencies which exercise investigative authorities and are responsible for preventing further damage; cooperation at the policy level which would facilitate quick understanding of the overall picture of an incident and necessary policy responses; information-sharing at the diplomatic level to avoid unexpected escalation into potential conflict; and cooperation among researchers engaged in research and development on leading-edge technology. Indian Government should actively work toward establishing a multi-layered global mechanism for information-sharing and will enhance its preparedness for the event of cyber incident.

12.3. Appropriate Response to Cybercrime International cooperation needs to be strengthened in order to effectively deal with cybercrime which easily transcends national borders. Indian government should continue to exchange information on cybercrime and digital forensics with foreign law enforcement agencies. India should also dispatch personnel overseas in order to exchange information on the latest cybercrime investigative techniques and to strengthen cooperation with overseas investigation agencies and should actively request mutual legal cooperation.

12.4 The Need for International Cooperation The case for international cooperation is even stronger, when criminals take advantage of countries' inability to coordinate, due to legal reasons or because authorities do not have the necessary technical expertise or resources to address the issue. Cybercrimes are not always clearly illegal in some jurisdictions. Further, it is easy to learn how to commit a cybercrime, which often needs few resources relative to its impact. Cyber attacks are independent of time and place. Cyber defence is hard as criminals are now in possession of rapidly renewable arsenals of attack weapons that can potentially cause global harm. Authorities must observe jurisdictional boundaries and due legal procedure while ensuring that the criminals are not given the scope to escape through loopholes. Further, cyber-criminals need to find a vulnerability to exploit, while ICT security professionals and software must guard against many different types of vulnerabilities. Due to increase in vulnerabilities, threats in cyberspace are growing rapidly. The rate at which new viruses emerge, the overwhelming presence of spam, the sophistication of phishing sites and the spread of implanted Botnets are all cause of concern.

Cyber criminals are no longer playful hackers, but are now well-organised in profitable conglomerates with substantial economic and technological resources. Cyber criminals are increasingly developing new attack software, which soon find its way onto the black market. Beyond profits, these groups may also be driven by more sinister motives for political gain. It is easy to imagine how Cyber terrorists or states or other groups intent on Cyber war can take advantage of the potential of these tools and software for causing damage.

XIII. RECOMMENDATIONS

Reaching to a common set of definition for cyber attacks, cyber espionage, cyber terrorism, cyber war, cyber crime etc. is the starting point. Which activities on the Internet (e.g. hacking, propaganda, attacking to

infrastructures etc.) should be counted as what must be defined exactly. Essential national and international legal measures have to be taken. International legal arrangements should be realised. The national legislation has to be harmonised with the international legislation. Both bilateral and multilateral agreements on cyber security cooperation should be signed among nations. An intelligence pool should be created in order to collect and share the intelligence simultaneously among the nations. Collecting intelligence should include not only monitoring websites of potential state and non-state actors but also collecting electronic evidence for the potential incoming cyber-attacks. The following are recommended:-

- A concerted mutually agreed strategy and policy should be constituted by member nations.
- Develop and accept common standards for sharing of data.
- Laws pertaining to cybercrime needs to be redefined to overcome legal hurdles. Adequate and flexible MLA and extradition arrangements must be there.
- Common set of investigative powers.
- Create an ecosystem of trust that may put the criminals and terrorists under pressure and increases the success probabilities of the international law enforcement agencies.
- The collection of electronic evidence whenever it relates to terrorism is crucial for the nations who desire to cooperate. Afterwards defensive and offensive (deterrence) collaborative actions should be set out.
- Counter information and cautions to the related public opinion and parties must be provided by the international organisations as defence strategies.
- Provisioning of Deterrence for all cyber crimes including cyber terrorism. The impact of deterrence is positively correlated with the identification probability and with punishment level.

It will be beneficial to have collaborations with International Cyber Security Protection Alliance, such as Australian Cyber Security Centre (ACSC), National Crime Agency's National Cyber Crime Unit (NCCU) and the UK's Child Exploitation and Online Protection Centre (CEOP). This will help in not only adopting the best practices by other countries for prevention of cyber crime, but also in increasing the capability, knowledge, training, skills, capacity and expertise of cyber security task forces. Additionally, it will help to reduce the harm caused to businesses, customers and citizens due to international cyber attacks. India should be actively engaged as part of the international cybercrime associations centred on Asia/Europe and America to seek help and contribute for international cybercrime issues.

XIV. CONCLUSION

It can be concluded that making the cyber world safer is of primary interest to all stakeholders. A secure cyberspace has become a very significant pillar for businesses to establish, operate and flourish in any region. The efficiency gains provided by the cyber domain are very valuable for mankind and using them for mutual destruction would be a serious folly. Once all nation states share this common perception, combating cyber crime and terror would not be an impossible mission. This could be achieved only through international cooperation and collaboration. Lack of trust and international political compulsions to use the cyber domain for projecting the state power have sabotaged this potential collective action against cyber crime. The use of Cyber Warfare as fifth domain in addition to land, Air, Sea & Space has resulted in all States developing their cyber deterrence capabilities targeted against their adversaries. This makes the task of identification of cyber terrorism

and those related to cyber deterrence by state sponsored actors very difficult. There is going to very soon a need to impose strict no first use policy type as exists for nuclear weapons as more and more peace time cyber espionage cases and cyber deterrence capability and capacity building continues.

REFERENCES

[1]. Emily Pehrsson" Making the grade,An international regulatory framework for cybersecurity"The Project on International Peace and Security.

[2]. Abraham D. Sofaer, David Clark, Whitfield Diffie "Cyber Security and International Agreements"

[3]. Sanjay Goel, Charles Barry "Information Sharing to Manage Cyber Incidents:Deluged with Data Yet Starving forTimely Critical Data".

[4]. Information Security Policy Council Japan "International Strategy onCybersecurity Cooperation".

[5]. Murat Dogrul, Adil Aslan, Eyyup Celik "Developing an InternationalCooperation on Cyber Defense and Deterrence against Cyber Terrorism"