CYBERSECURITY- ITS EFFECTS ON NATIONAL SECURITY AND INTERNATIONAL RELATIONS

B. Venkatraman & Karun Gupta[*]

INTRODUCTION

Development of Cyber Policy

The concept of Information and Communication Technologies (ICTs) and cyber laws all over the world is relatively new in comparison to the rest of the laws that are legislated. With 1990s seeing its infancy with only a handful of people being able to access the internet compared to over 40% of the world population as on 2014, one can see how ICTs have grown rapidly on a daily basis over a short span of time.

As this aforementioned concept is relatively new one, legislating laws in order to regulate activity in this vast borderless space is a challenge since traditional legal systems and laws are not modern enough to keep pace with this rapidly progressing mode of communication. The unchecked incidences of cyber-crime has led to hindrance to the daily activities of people, both commercial and personal, as well as pose a threat to the securities of nations at national or international level. Taking the example of India- a nation heavily dependent on this technology, a notification issued by the Ministry of Communications and Information Technology (Department of Electronics and Information Technology) in one of its paragraphs states that: *"Information Technology is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (government* *to citizen services, citizen identification, and public distribution systems), Healthcare (telemedicine, remote consultation, and mobile clinics), Education (e-learning, virtual classrooms, etc) and Financial services (mobile banking/payment gateways), etc. Such initiatives have enabled increased IT adoption the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate/private participation".*[1]

Up until the last 10 years Cyber policies remained more or less in the background of policy making. Even before 9/11, a number of exercises identified apparent vulnerabilities in the computer networks of the U.S. military and energy sectors. After 9/11, the security and terrorism discourse soon featured cyber-terrorism prominently, promoted by interested actors from the political, business, and security circles.[2] This brought cyber policies into the limelight as it then became one of the most key issues in politics. The global, often non-transparent interconnections afforded by cyberspace have challenged the traditional understanding of leverage and influence, international relations and power politics, national security,borders, and boundaries — as well as a host of other concepts and their corresponding realities.[3]

Owing to all the powers and responsibilities that are offered by ICTs and the cyberspace, it leads to a speculation on the vast scope that is there for policy making regarding this field. This gets fuelled by all the activities that encompass the field of international politics i.e. legislation, negotiation between parties with regard to rights, responsibilities and procedures, creates new opportunities for states to engage with each other more often, communicate their needs and concerns and also work together. This on the larger scale brings about a change in the nature and needs of a state as a caretaker of its people.

For example, the need of a state and its population has been talked about in Adolf Hitler's *Mein Kampf.* It says that for a state to grow as a world power it will need to bring more land within its control which would allow it to produce and export more. However, with the advancement of technology especially the ICTs, it resulted in capital becoming more and more mobile thus making it possible for production and transactions to be done abroad. As a consequence this went on to increase the

* Authors are students of Amity Law School Delhi affiliated to GGSIPU

[1] Notification on NATIONAL CYBER SECURITY POLICY-2013(NCSP-2013),File No. 2(35)/2011-CERT-In, http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

[2] GABRIEL WEIMANN, CYBER-TERRORISM-HOW REAL IS THE THREAT?

[3] NAZLI CHOUCRI, CYBERPOLITICS IN INTERNATIONAL RELATIONS 3 (2012).

importance of knowledge, technology and capital and reduce the importance of land. The state no longer commands resources as it did in mercantilist yesteryear; rather, it negotiates with foreign and domestic capital and labour to lure them into its own economic sphere and stimulate its growth. The virtual state also locates production overseas so that it can concentrate home efforts on high-level services: research and development, product design, financing, marketing, and transport.[4]

CYBER-POLICIES IN ASIA

As aforementioned, it is the internal policy of the state that dictates its relations with other states and the international community at large. Keeping this in mind some of the policies of states with regard to ICTs, their use and to prevent misuse are examined with emphasises on how these states utilise the technology.

China

A recent giant in the ICT sector China since 1997 has prioritised ICT development which has made the state one of the largest players in the telecommunications market. Its IT industry has been an engine of economic growth - growing two to three times faster than GDP over the past 10 years[5]. In order to simplify, China has been referred to as a homogenous entity.

In order to fight criminals and counter terrorism the government drafted several laws in the year 2015. These laws mostly involve security checks over systems and data storage within the country. One such example is the example of the National Security Law which was passed on July 1st, 2015. As per Article 1 of this statute, the statute itself had been enacted in accordance with the constitution so as to *maintain national security, to defend the people's democratic dictatorship and the socialist system with Chinese characteristics, to defend the fundamental interests of the people, to ensure the smooth implementation of the reform and opening up and establishment of socialist modernization and to realize the great revival of the Chinese nationality.* The rules for combating defaulters are framed in such a way that the body tasked with this responsibility is able to track them even before the crimes are committed. For example section 3 of the aforementioned statute comprising of articles 55 to 58 allow governing bodies even at the county level to investigate and report to the people's government of any threat to national security

[4] Richard Rosecrance, *"A New Kind of Nation" in The Rise of the Virtual State* 5 (Barnes & Noble, 1999).

[5] CHRISTINE ZHEN-WEI QIANG, CHINA'S INFORMATION REVOLUTION: MANAGING THE ECONOMIC AND SOCIAL TRANSFORMATION 35 (2007).

that might occur. Section 4 grants enormous powers to the national security review boards to scrutinise foreign commercial investment, special items and technologies, internet information and technology that might pose a threat to the national security of the nation. The act grants enormous powers to the authorities by leaving most of the procedure undefined and largely leaving decision making to the authorities and inadequately defining the remedies.

However, Chinese officials say the measures are necessary for national security, allowing them to verify that critical equipment isn't vulnerable to hacking and to help them track down criminals and fight terrorism. But the rules have been criticized by foreign governments and trade groups as onerous and a possible way to discriminate against non-Chinese vendors.[6]

Pakistan

Despite strides taken in the cyberspace world and the advantages it offers Pakistan still lags behind in the field of cybersecurity. Due to various lapses in procedural and legal mechanisms to prevent cyber-terrorists, cyber terrorism has become rampant in the nation. Hacktivism is unchecked in Pakistan, and in present time period there are number of Pakistan's government official sites that are being defaced by hackers and the government is totally helpless in countering them, because of not having advanced technology to prevent these cyber-attacks[7]. However, in April 2016 the nation saw the passing of the Prevention of Electronic Crimes Bill in order to combat threats to national security. This act involves the designation of a Federal Investigation Agency that shall have powers defined in the act itself for the procedure to conduct investigation and present it to the authorities. The bill in chapter II grants powers to the specialised investigation agency officers regarding search and seizure of information stored in servers which if the officer feels is required for the purpose of a criminal investigation or that which may have been lost, modified or rendered inaccessible later on and may issue a notice to the holder of such data to protect integrity of such data. The bill has been criticized by the IT industry and the civil society for 'curbing human rights and giving overreaching powers to law enforcement agencies'.

According to the bill, hacking as well as interference with data and information systems, specialized cyber related electronic forgery and electronic fraud, cyber terrorism (electronic or cyber-attack on the critical information

[6] Eva Dou, *Untangling China's Cyber security laws*, WALL STREET JOURNAL, (Jun 03, 2016), http://blogs.wsj.com/chinarealtime/2016/06/03/untangling-chinas-cybersecurity-laws/.

[7] SADIA RASOOL, CYBER SECURITY THREAT IN PAKISTAN: CAUSES CHALLENGES AND WAY FORWARD 4 (2015).

infrastructure), unauthorized interception conducted by civilians, use of malicious code viruses, glorification of an offence, hate speech, identity theft etc. have been declared punishable offences. According to clause 10 about cyber terrorism, anyone advancing religious, ethnic or sectarian discord or involved in creating a sense of fear, panic or insecurity in the government or the public shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine up to fifty million rupees or with both[8]. The bill also authorises the government to cooperate with a foreign state entity with regards to investigations regarding offences related to ICTs and collection of electronic evidence.

Afghanistan

The development of ICTs in Afghanistan was able to start only after the establishment of the interim government in 2001. However, considerable progress has been made between the years 2002 -2012, starting from an almost total absence of internet in 2002 in the country to almost 44 internet service providers with an internet subscription population of nearly one million and Mobile telephone penetration in the country surpassing 80 per cent of the population[9]. In 2009 The Ministry of Communications and Information Technology (MCIT) established the first Cyber Emergency Response Team which was officially named as AFCERT. Its duty was to fight against cyber threats and crimes and provide awareness and solutions on cyber security to the government and private sector. In its first two years of operation, the team reported an increase in cyber and electronic related crimes to its parental department in the country. Based on a report it had prepared, the MCIT and the ICT council established a committee whose purpose was to fight the aforementioned crimes. It is expected that by 2020 MCIT will become an independent entity within the government so as to prevent unwarranted influence on it from other entities. Analogous to the international cooperation policies in Pakistan the MCIT also has the power to aid other states in the tracking down of cyber criminals. However it does not have as much authority as the former with respect to sharing information with the international community.

India

Despite having IT laws enacted way back in 2000. This IT act of India, amended subsequently in 2008, barely had a few sections

[8] Zahid Chaudhary, *NA approves cybercrime bill*, PAKISTAN OBSERVER, (Apr. 14, 2016), http://pakobserver.net/na-approves-cybercrime-bill/.

[9] DRAFT NATIONAL ICT POLICY (AFGHANISTAN), http://mcit.gov.af/Content/files/Draft%ICT%20Policy%20Document.pdf.

which classified offences into the civil offences and penal offences only. This however was not enough for the private companies which had to resort to self-regulation and entering into contracts with cyber-security providers. Cyber-security in India was not developed until the aftermath of 2009 which can be attributed to the infamous cyber-espionage operation brought to light by the Information Welfare monitor named "GhostNet". It emerged that computer systems belonging to ministries, embassies and other government offices of India, among others, were infiltrated and sensitive documents were exfiltrated[10]. No substantial changes in the IT act have occurred. The IT Act itself has been riddled with a controversy, specially section 66A which aimed at punishing those who electronically posted "objectionable" content. This objectionable word was never defined thus turning into something which was always abused by the authorities giving them autocratic powers, not unlike China, until it was repealed a year ago.

When it comes to cyber-attacks, India unlike all the above described countries does not have a body that is dedicated to combating these attacks. Seeing this as a problem, the National Cyber Coordination Centre was created under the directions of the National Cyber Security Policy 2013. This centre is supposed to work by scanning information metadata and acts as a coordinating body for other intelligence agencies like IB, RAW, CBI.

Democratic People's Republic of Korea

One of the most significant actors in the field of ICTs and cyber-securities is North Korea. Their activity can be attributed to both its military and intelligence organisations, having gained the abilities to conduct cyber operations testimony to which is the 2014 attack on Sony pictures. DRPK cyber strategies and operations are managed by the Reconnaissance General Bureau and the General Staff Department of the Korean People's Army. It is difficult to pinpoint exactly how advanced North Korea's technical capabilities are given the paucity of available open source analysis. Certainly, they have evolved beyond rudimentary DDoS attacks against websites they have often resorted to in the past decade, into more targeted, complex, and well-organized operations involving several stages of exploitation of a target system or network. They are capable of social engineering, extended advanced persistent threat campaigns, and employment of less sophisticated but sufficiently effective malware such as the Jokra wiper tool observed on March 20, 2013. South Korean media reports that North Korea has

[10] SRIJITH K NAIR, THE CASE FOR AN INDIA-US PARTNERSHIP IN CYBER-SECURITY.

started to target smartphones as well. Contrary to popular assumptions, North Korea maintains a fairly competent computer technology base including the Korea Computing Center (KCC) and the Pyongyang Informatics Center (PIC) as well as several universities such as Kim Chaek University of Technology and Kim Il Sung University's School of Computer Science. They allegedly have additional military-related institutions to specifically train individuals for cyber operations.[11]

Republic of Korea

Ever since ICTs came into mass usage in South Korea the nation has been subject to many cyber threats and attacks from North Korea thus most cyber security measures that were taken up were a reaction to either a threat that came from North Korea or from the fear of an internal governmental department. South Korea established two main agencies to unify its cyber-security efforts: the National Cyber Security Center (NCSC) led by the National Intelligence Service (NIS), and the National Cyber Command (NCC) led by the South Korean military. The South Korean military and NIS played key roles in supporting authoritarian regimes in South Korea's past. Consequently, South Koreans are worried about the concentration of authority in the NCSC and NCC. Moreover, a few agents in the NIS and NCC have been suspected and accused of engaging in intervention in domestic politics during the last South Korean presidential race in 2012.[12]

Thus, this combination of fear and pressure is increasing the distance between the government and various civil societies in that nation which later goes on to slow down the progress which the nation is capable of making in the field of cyber-security which can not only make it easier to trace and prevent the hacks that are happening on their society but also can go on to take measures wherein the government may be able to increase the transparency thus allowing their general public to trust them more.

Cyber Technology Vis A Vis National Security

As the economy of the world becomes more and more dependent on the use of the internet space for purposes such as banking, online transactions, storage of information both private and governmental a certain risk is created at the same time which threatens this "cyber" way of life. Problems such as cyber-terrorism, hacktivism (Anonymous) and governmental cyber-espionage operations

[11] JENNY JUN, WHAT DO WE KNOW ABOUT PAST NORTH KOREAN CYBER ATTACKS AND THEIR CAPABILITIES?

[12] *Cyber Security Spotlight: South Korea*, JACKSON SCHOOL OF INTERNATIONAL STUDIES, (July 23, 2016), https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/.

(Stuxnet) have increased over this decade owing to this very dependence on cyber technologies. Naturally, states would react by taking up various measures that increase security in this sphere. In order to go about this a state naturally would first and foremost consider in which sphere of the cyber-world the stakes are the highest. Once this is found it will have to conduct an analysis of the nature of this sphere by finding out from where and whom these threats lie, how that particular entity could cause damage to that sector, etc. On the discovery of such information it will have to see where all of these threats call for the formation of a specialised intelligence agency or whether the general intelligence agency is capable enough to handle this security. Once these plans are in place implementation becomes a whole new task for the nation. To achieve this, ideally a state then forms public private partnerships with corporations that specialise in such services; they may also achieve this by spending more on Research and Development (R&D) in technology that aide in bolstering cyber-security. All of this, which has to be done keeping in mind the basic fundamental values a nation stands for be it the safety of people(at the cost of liberty itself) or the liberty of the people or both but the goal of the state remains the same in the end i.e. the safety of the people.

Before coming to the various needs and intricacies of the current cyber-security policies and how it is linked to both national security and international relations a question comes up as to how could a completely new sphere in laws and policies develop in such a short span of time? The answer to that is the fact that the usage of a resource and the evolution of the laws that regulate its use go hand in hand. For example when the laws governing air rights only became substantial when the world realised its true potential as a public resource and how vital it is for the economy. Similarly, as the usage of the cyberspace grew from catering to the needs of just a few elite people and entities the need for that hour was just to prevent any kind of injury that could be caused to these people by the misuse of this resource. But as the internet and all the benefits that came along with it grew and also went on to cater to the needs of the common man it became imperative for the state to take measures that protect this cyber-dependant society as a whole and not merely protect the few individuals. Taking an example, the Computer Fraud and Abuse Act 1986 which in its infancy merely aimed at punishing hackers was something which was deemed suitable to that era but certainly would not have been enough after 2003 due to which enforcement bodies such as the National Cyber Security Division of the Department of Homeland

Security which were dedicated to prevent the misuse of this cyberspace which the common man became reliant on.

Keeping in mind what was said earlier, this change in the role which this cyberspace plays and how the policies regulating its usage have also changed it becomes imperative for a state whose infrastructural development is heavily subjected to the use of ICTs to also make that transition from a method of fragmented policy making to a policy making on a more extensive level i.e. the method of restricting laws and usage related to the cyberspace merely at a military level is a thing of the past. Therefore in order to develop as a whole the state will have to make use of the economic advantages the ICTs have to offer, this is because most of the cyberspace is owned and operated by the private sector and time and again it has been shown that it is this private sector that improves the standard of living of the people thus it means that the states will have to make policies that favour these businesses, civil societies, the Internet technical communities, etc which goes on to strengthen the economy. Now, as the economy of this nation grows owing to the use of the cyberspace this means that there would also be a rise of malicious agencies like hackers, online frauds, cyber-terrorists, other hostile states which seek to jeopardise the development of that state and its people for its own purposes by targeting its infrastructure. This calls for the state to now make use of the law enforcement and military intelligence aspects which the cyberspace has the potential to provide which means the state will have to allocate a significantly large portion of its budget to increasing its cyber-security. This however is aperfectionistic assumption, it is so because most states are reluctant to implement measures that increase their national security at the cyber level because:

- **Complacency** – It is only seeing the recent mass attacks by various entities that states have decided to work on their cyber-security. Following the rise of the internet and post 9/11 attacks, despite knowing that the cyberspace is one strategic front which also needs to be defended just like the airspace and territorial waters states still fail to recognise the importance or take up half measures either by enacting vague cyber laws or delegating powers of enforcement to a body without analysing its consequences on the body itself and the people. It is only a mass cyber-attack which usually serves as a wakeup call for nations to finally do something about their cyber-security. *"South Korea on Monday outlined a nationwide cyber security strategy following a series of recent online attacks on state-run and corporate websites, including net* *offensives allegedly launched by North Korea. The country`s move comes as the latest incidents of cyber-attacks and online data theft around the world pose greater threats to both the private and the public spheres, prompting global state actors, including the United States, to devise a new government-led strategy to beef up their net security."*[13]Clearly it can be seen here that the move to increase cyber-security was the result of an attack done and not the result of preparedness by the state.

- **Volatility**- Volatility can be in the form of instability which is in the state itself i.e. due to war, unrest, etc. when this happens the question of cyber-preparedness becomes a moot point. But in other cases this volatility is something that exists in the government especially in one of a multi-party democracy. Seeing the case of India, which is an apt example of a volatile nation with a volatile government, the fact that there is a change every 5 years means that there will be governments which are more liberal in nature and governments which are more pro security. This hinders the creation of a policy which creates definite set of cyber-security norms and rules with political power plays being the reason for the formation of a hasty policy and not the benefit of the people. A state with a volatile government, in order to put into effect a cyber-defence which is strong enough to keep up with the current hacking trend must delegate to a body consisting of people with specialised knowledge in the subject in order to propose an effective defence policy and judicial officers so that these policies are not contravening to the constitution of the nation.
- **Effectiveness Gap** –One of the most disturbing trends seen in nearly every cyber-security defence system is the gap between the defences and the attacks. "*The modern cyber-security architecture of secured networks, firewall protection and anti-virus on endpoints does not seem to be holding up well against cyber-attacks consisting of protocol tunnelling, spear phishing and zero day attacks on endpoints and servers alike. Infact, given the complexity of modern devices, exploding size of modern IT enterprises, interconnections between vendors, partners and customers even maintaining the defence of 10 years ago is a surprisingly daunting task for professionals."*[14]

[13] *S. Korea charts out national cyber security strategy*, ANTARA NEWS, (July 24, 2016), http://www.antaranews.com/en/news/74600/s-korea-charts-out-national-cyber-security-strategy.

[14] ABDUL ASLAM, CHRIS K. WILLIAMS, SCOTT E. DONALDSON & STANLEY G. SIEGEL, ENTERPRISE CYBER-

This leads to a conclusion that the cyberspace is an area that is evolving at a far more rapid pace than other spheres which means that the state defending its cyberspace cannot simply enact a defence and security policy and sit back. In order to be able to withstand the countless attacks that happen the state will have to keep checking and updating its security defence systems on a regular basis.

A caveat to all the states seeking to protect its cyber-defences is that the laws, rules, and procedures it will mandate in order to protect the same must be in accordance with the constitution of that nation. Nations such as India only recently amended their laws to promote free speech in the case of *Shreya Singhal v. Union Of India*[15]. Although the case was relating to posting offensive content on electronic media since the particular statute was against the principles of the Constitution of India it had to be amended. Similarly the state enacting laws to protect its cyber defences must ensure that this protection does not turn out to be repressive in nature as such repressive laws will only go on to increase the distrust between the public and the government which will in turn call for more repressive laws thus the state will no longer be doing the role of a welfare state but that of a police state. Taking the example of one of the earlier mentioned states South Korea is a nation that faces constant threat of cyber-security attacks from North Korea and as a result the NIS and the South Korean military had to take charge over defending the nation's cyberspace but a problem that arises in this is that due to the past of these organisations with the authoritarian regimes there a fear is created in the minds of the general public of the possibility of such a situation repeating itself. This puts the government on thin ice regarding the framing of laws regarding this front thus emphasising on the point on how the rules regarding control of such devices should be so that they not only offer adequate protection but are not in such a way that they encroach on the rights of the people *"Self-defence" provisions in current law already authorize communications companies to share incident information with the government in order to gain assistance in responding to a cyber-attack. Instead of empowering the government to seize such information from companies or monitor private networks for attacks, incentives should be developed to encourage companies to share this information*[16].

SECURITY: HOW TO BUILD A SUCCESSFUL CYBER-DEFENCE PROGRAM 21-22 (Apress 2015).

[15] (2013) 12 SCC 73.

[16]GREGORY T. NOJEIM, CYBER-SECURITY AND FREEDOM ON THE INTERNET.

Thus making the cyber-security program more transparent will built the confidence and trust that is essential for this industry and for a government to ensure stability in the state.

Cyber-Security and International Relations

Coming to the more extensive aspect of cyber-security is, how it affects international relations. The effect use of cyberspace has on the relations between states is far more than other internal policies can have. This can be attributed to what was said earlier i.e. the present role of this cyberspace. Cyberspace being a medium has always existed to connect to entities thus making any interaction between them progress at a much faster rate thus when the access to cyberspace arrived at the doorstep of the common man the internet itself became a device of mass communication that too which can occur between people across the borders as well. Owing to the aforementioned reason cyberspace and its protection became something which is capable of affecting states and their relations with each other.

As cyber offense and defence capabilities continue to develop rapidly, the complexity of maintaining international relations will go on increasing but some challenges which this aspect of cyber-security faces is firstly how owning to the recentness of this concept there are no set guidelines governing the use of this medium unlike the guidelines for the use of the seas and the air there exist none for cyberspace. Arising from the first is the second challenge i.e. owing to the lack of guidelines it becomes easy for nations to involve themselves in cyber-attacks against their fellow nations as it is difficult to bring direct conclusive evidence against that.

"A powerful example to illustrate this is the Stuxnet virus, which was programmed to damage Iran's centrifuges at the Natanz nuclear site (Rid, 2012). While Israel and the U.S. have been blamed as creators of the virus, the nature of the cyberspace makes it impossible to trace the actual origin of the software[17]*."* Thirdly, owing to this particular nature of the cyberspace where it becomes a cumbersome process to track an offender, nations tend to attack more via this medium than the others. An example of which can be seen through the attack on Sony pictures in 2014 the suspicion of which is on North Korea. Furthermore, the actions of John Snowden and Julian Assange where they have acted as a whistle-blower exposing several acts by the US government has triggered a game of politics between nations such as USA and its rivals China & Russia where on one hand

[17] NirKshetri, *Cybersecurity and International Relations: The U.S. Engagement with China and Russia* (Paper Presented at the FLACSO-ISA 2014 Buenos Aires, Argentina, July 23-25, 2014)

Snowden has been declared as a traitor but has been praised by and granted asylum by the others. This goes on to complicate the already complicated relations between the three nations all of which is owing to the use of this cyberspace.

Despite its hindrances there have been several occasions where treaties have been formed owing to the purposes of cyber-security for example the partnership between United States Secret Service, Italian Ministry of Internal Affairs and Poste Italiane established in 2009 which consists of both public and private organisations that aims at preventing crimes in the EU. On another occasion China in partnership with the FBI has been able to shut down a website dealing with child pornography in 2011. Seeing these examples one may note that the cooperation regarding cyber-security only comes when there arises a conflict of interests between some states and another entity. Thus, for a state which seeks to better its relations with another state without having to compromise much on its own interests it may do so by extending cooperation in the form of providing defensive measures in the cyberspace and helping with tracking down cybercriminals. In light of all of this it can be concluded that the international ramifications of cyber-security is still at a fledgling stage. It can be seen that for international relations to develop a state will have to hand a certain degree of cooperation and to do so it will have to frame its cyber-defence rules accordingly but while doing so it must fathom whether in doing so is it compromising on its critical national interests, its national security or any other sphere which is vital to its development? After this is seen naturally, in most cases the cooperation will be a cold one where nations would be wary of each other and it is at this stage where working together can prove to be a do or die effort for the relations between the states.

CYBER-SECURITY: CONCLUDING REMARKS AND THE WAY AHEAD

As emphasised upon earlier, ICTs in the cyberspace have been one of the most rapidly advancing technologies in the past few decades, this paves the way for an increased number of opportunities in both economic, military and social spheres of development and where there is road for development there is always an entity seeking to work for its own benefit at the cost of that of others. The Global State of Information Security Survey 2015 was conducted by PwC, gathering responses from more than 9,700 security, IT, and business executives in 154 countries.

“The research found that the number of detected information security incidents has risen

66% year over year since 2009. In the 2014 survey, the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48% from 2013—an average of 117,339 per day."[18]

Making matters worse the most threats that occur are by the state backed entities which seek to disturb the critical infrastructure such as oil and gas, energy, military and telecommunication sectors. Since most critical information is stored there the attacks will begin there which will go on to steal all this information making the nation's defences predictable. Thus, a requirement is created to allocate more funds for defence on the cyber-security front.

The state defending its cyberspace can no longer afford to prepare for action after the damage is done rather it will have to focus on preparing its defences in such a way that the attacker is delayed and so that it can cooperate with other states if necessary.

Cyber technology is a double edged sword which needs to be handled carefully. If at such an early stage it is proven to bring economies at a standstill then the possibilities of it causing far more damage develops as it more and more becomes a part of our lives.

[18] *Cyber-attacks upto 48% in 2014*, CGMA MAGAZINE, (July 30, 2016), http://www.cgma.org/magazine/news/pages/201411089.aspx.