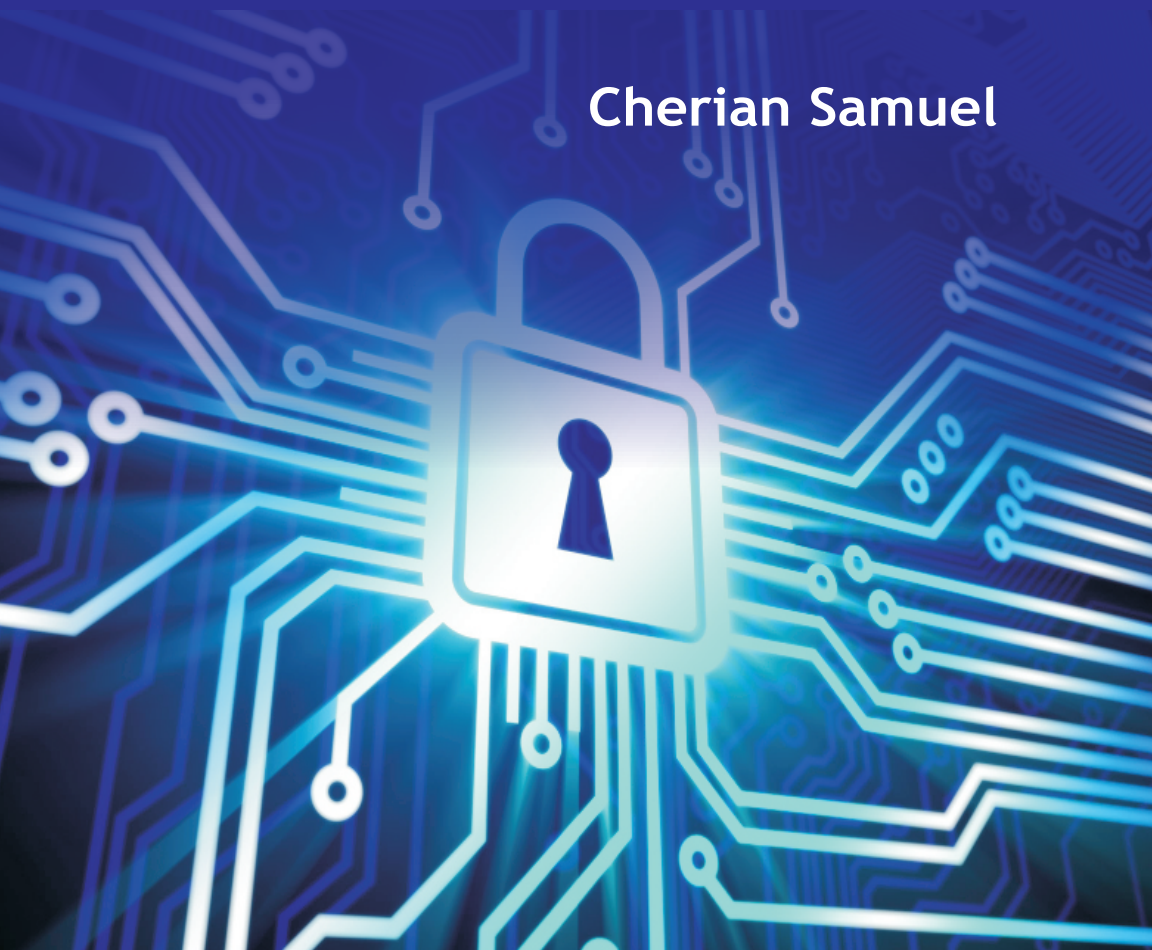
IDSA Monograph Series
No. 42 December 2014

# Cybersecurity

## Global, Regional and Domestic Dynamics

Cherian Samuel



IDSA Monograph Series
No. 42 December 2014

# CYBERSECURITY

## GLOBAL, REGIONAL AND DOMESTIC DYNAMICS

Cherian Samuel

INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

**Cover Illustration Courtesy::** http://www.shoreline-solutions.com/debit-credit-card-personalization-services-blog/wp-content/uploads/2012/10/cybersecurity_11.jpg



ISBN: 978-93-82169-48-2

*Disclaimer:* It is certified that views expressed and suggestions made in this monograph have been made by the author in his personal capacity and do not have any official endorsement.

First Published: December 2014

Price: Rs. 225/-

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983 Fax.(91-11) 2615 4191
E-mail: contact.idsa@nic.in
Website: http://www.idsa.in

Cover & Layout by: Geeta Kumari, Vaijayanti Patankar

Printed at: M/S A. M. Offsetters
A-57, Sector-10, Noida-201 301 (U.P.)
Mob: 09810888667
E-mail: amoffsetters@gmail.com

# Contents

*CHAPTER - 1*

# INTRODUCTION

Fourteen years into the new millennium, governments find themselves struggling to deal with the issue of cybersecurity. What promised at the beginning of the century to be a set of technologies, which would facilitate economic growth and the advancement of knowledge, is now considered by many governments as having spawned a domain that is anarchic and in dire need of control and regulation. And not without reason; cyberspace is being used for a variety of malicious activities, from crime to state-sponsored attacks on critical infrastructure. The interconnectedness of cyber networks means that even the most basic responses end up having a ripple effect or unintended consequences. Maintaining a balance between security and benefitting from the many opportunities provided by the deployment of new cyber technologies is proving to be one of the most vexatious issues of the 21st century.

The complex nature of cybersecurity has seen even the developed countries of the West, where many of the technologies, processes and practices were developed, falter when it came to developing holistic cybersecurity policies. The countries that succeeded in piecing together a policy have had difficulties in implementing them, and have also had to come up with successive iterations as new threats have surfaced. Such policies have also been of limited use in preventing cyber attacks or for pre-empting new threats.

While India was among the first countries to have an Information Technology Act, set up a Computer Emergency Response team (CERT) and even locate responsibility for cybersecurity within the National Security Council, it has subsequently lagged behind other countries in responding to cybersecurity threats.

India has been at the receiving end of various forms of cyber threats; from attacks on critical infrastructure to cybercrime and the latest manifestation of the misuse of social media. Moreover, responses at the official level have been marked by several mis-steps. Till recently,

there was an inadequate appreciation of cybersecurity threats at the official level though that is no longer the case.

Given the current state of play in cybersecurity, it is not surprising that any discussion on cybersecurity sooner or later ends up as a confusing mix of viewpoints on fundamental rights, privacy, law enforcement, human rights, globalisation and national security, thus leading to a gridlock. With the passage of time, differing perspectives and approaches are getting more and more entrenched, thus making the job of arriving at a consensus on contentious issues even more difficult. The resultant disarray has emboldened a variety of malicious actors (state, non-state and criminal) to take advantage of the situation.

The confusion at the domestic level is reflected and magnified at the international level with various countries having different approaches and cybersecurity priorities. At the same time, the threats and perceived threats have led many countries to go beyond a merely defensive architecture and advocate more pro-active and offensive approaches to be pursued by agencies with expertise in civilian, military and intelligence domains.

One of the problems plaguing any discussion on cybersecurity is the vast gulf between the practitioners, and policy makers in experience, understanding and perception. Though cyberspace is now a near universal phenomenon, it has touched different countries at different points in time, and its usage has also differed across countries. This has led to differing perceptions of cyberspace and its intricacies, which explains why, even as the medium acquires strategic significance, most countries are finding it difficult to articulate a strategic perspective that both maximises utility and assures security.

This monograph begins by tracing the history of the domain, which has impacted its development as well as the various issues that play a part in its functioning and need to be understood to contextualise the issue of cybersecurity. While the history is covered in Chapter 2, Chapter 3 examines India's approach through this lens. Chapter 4 analyses the future of cybersecurity by studying the unfolding cybersecurity scenario in Asia, which in many ways is at the frontline for cybersecurity threats. Chapter 5 looks at priority areas that have to be addressed in the Indian context.

*CHAPTER - 2*

# FACTORS AND ACTORS IMPACTING THE PAST, PRESENT AND FUTURE OF CYBERSPACE

The discourse on cyberspace is impacted by its past, present and various perspectives on the future shape of cyberspace. Though clearly a global phenomenon, national, regional and even individual perspectives are largely determined by various factors operating across time and space. As such, no discussion on cyberspace would be meaningful without a study of its history, the various perspectives on it and the various actors in this sphere.

## History of Cyberspace

The history of cyberspace is a continuing story of the incremental and disruptive advancement of a number of technologies.[1] Its early days presaged many of its current applications. It was initially envisaged as a means of communication among academicians across various academic institutions, so much so that the various innovations that propelled it forward can be traced to individuals who improved on the original system. This also explains why one of the problems facing cyberspace today is the lack of adequate security protocols.

The initial impetus was provided during the Second World War when the largest conglomerations of scientists ever, came together at Bletchley Park in the 1940s to break German encryption codes. The cross-fertilisation of ideas that occurred there was disseminated across different scientific institutions after the war, and these collaborative efforts continued to maintain the momentum of the great spurt in

---

1 "*Brief History of the Internet",* Internet Society (Undated), at http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (Accessed November 1, 2012).

scientific development that was partly the by-product of the war effort.[2] Communication between institutions was an expensive affair since costs were based on distance, and dedicated lines required to transfer data were prohibitively expensive. Despite that, many networks were established between institutions, but the technology to transmit data remained primitive, with messages sent on the store-and-forward principle taking time to reach their destination. Theoretical alternatives began to make their appearance in the early 60s with the first paper on what was to become the mainstay of cyberspace, the 'packet switching theory', being published in 1961. The first system based on this theory, the Advanced Research Projects Agency Network (ARPANET), was developed by the US Department of Defence Advanced Research Projects Agency (DARPA) by 1967. DARPA's interest in technology was based on the need to develop a communications network that could survive a nuclear war. While the ARPANET was a single network, other scientists began work on facilitating communication between networks leading to the development of Transmission Control Protocol/Internet Protocol (TCP/IP) in the 1970s.

The ARPANET connected various universities, research institutes, and scientists and was further improved throughout the 60s and 70s. The Local Area Networks (LANs), mainframes, and personal computers led to increasing use of these networks, which in turn increased the demand for these devices. Since the data had to be transferred between the supercomputers of the time, a premium was placed on increasing the speed of data transfer. As universities became the largest users of the facility, the National Science Foundation took over and instituted the National Science Foundation Network (NSFNet), which became the Internet backbone and was utilised by the smaller networks.

The Internet flourished because of its underlying simplicity. It consisted of just four layers, each focusing on one aspect of data flow.[3] Data was split into packets, and transmitted on a best effort basis, with the various layers ensuring that the data arrived at its final destination by a

---

[2] Stephen Little, "From Bletchley Park to the NSA: Scientific Management and 'Surveillance Society' in the Cold War and Beyond", Unpublished Paper Presented at the Critical Management Studies 3 Conference, Lancaster University, July 7-9, 2003, at http://www.stephenelittle.com/cms03.pdf (Accessed 8 May 2013).

[3] The four layers were: Application, Transport, Internet and Link.

variety of routes and was reassembled successfully. This marked a fundamental departure from earlier networks that emphasised point-to-point connectivity, and were therefore tremendously expensive to operate since cost was estimated on the basis of distance. An alternate system, the Open Standards Initiative (OSI) floundered because it was just slightly more complicated.[4]

The networks stayed within the domain of academia till the 1990s when commercial usage was allowed, with the first Internet Service Providers (ISPs) enabling the general public to connect over dial-up networks. Another innovation that took place concurrently with this development was the invention of the World Wide Web at the European Organisation for Nuclear Research (CERN) by Tim Berners-Lee and Robert Cailliau. The development of applications like browsers and hyperlinking made the easy consumption of data possible. The fact that the earliest browsers such as Mosaic were free applications enabled their wide adoption. Competition ensured that these browsers, even when developed by commercial enterprises, continued to be free which allowed easy access to the Internet. Commercial networks developed apace with academic and governmental networks. Every successive development in the technology ensured that the networks became more and more interconnected leading to economies of scale resulting in reduced costs.

The next step in the evolution of cyberspace came about when it began to be used for e-commerce. While the early mass usage of cyberspace was mainly for basic activities such as e-mail, e-commerce became a major activity in the late 1990s. E-commerce did not take off overnight, but was popularised by activities such as online gambling and pornography. The latter was also partly responsible for popularising video over the Internet.[5]

Thus, the expansion of cyberspace is the outcome of the economic development in many areas, coupled with the incremental and

---

4 Andrew L. Russell, "OSI: The Internet that Wasn't", *IEEE Spectrum*, July 29, 2013, at http://spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt (Accessed October 25, 2013).

5 "Thank You, Porn! 12 Ways the Sex Trade Has Changed the Web", December 21, 2008, at http://www.pcworld.com/article/155745/porn_on_the_web.html (Accessed May 8, 2013).

continuous evolution of the technologies associated with cyberspace. While the core technologies were developed by the academia, the associated industries that developed side-by-side included personal computers and networking technologies. Another important element was that the standardisation of the various web technologies avoided the potential balkanisation of the Internet, a foregone outcome had these technologies been proprietary.

## *Threats in Cyberspace*

While threats have existed right from the early days of cyberspace,[6] the sporadic nature of the attacks and their targets suggested that they were largely the handiwork of hackers and low-level criminal elements. The major delivery vehicles were spam mails containing viruses and malware. These were however manageable and up-to-date antivirus programmes and firewalls were deemed sufficient for keeping such risks at bay. Subsequently, new forms of malware such as Worms and Trojans, which exploited the vulnerabilities of buggy software, also began to make their appearance. Phishing and Denial of Service (DoS) attacks also entered the lexicon. Whilst the former was a technique for gaining personal information for purposes of identity theft or access to e-mails or bank accounts, the latter consisted of malevolent attacks on websites with the intention of making them inaccessible. All these threats[7] took advantage of the existing vulnerabilities[8], whether in the software, networks or security architecture.

---

[6] For a detailed run-down of cyber threats from the early days of the Internet, see: Jason Healey, "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012", *Cyber Conflict Studies Association*, 2013.

[7] The Computer Emergency Response Team (CERT) in 1993 defined a threat as: "Any circumstances or event that has the potential to cause harm to a system or network .That means, that even the existence of a(n unknown) vulnerability implies a threat by definition."

[8] Vulnerabilities are defined as a) a feature or bug in a system or programme which enables an attacker to bypass security measures, b)an aspect of a system or network that leaves it open to attack and c) the absence or weakness of a risk-reducing safeguard which had the potential to allow a threat to occur with greater frequency, greater impact or both.

Anil Sagar, "An Overview to Information Security and Security Initiatives in India", PowerPoint Presentation, January 18, 2008, at www.elitex.i**n**/paper2008/a**n**ilsagar.ppt *(Accessed March 21, 2012).*

Criminal networks have, over the years, professionalised the business of discovering and exploiting weaknesses in software that allow them to undertake a variety of actions ranging from taking control of those computers, accessing information on those computers or rendering them unusable. Whilst hackers provide the technical expertise, existing international criminal networks have learnt how to squeeze the maximum out of these compromised computers, and have turnovers estimated in billions of dollars. With online and mobile banking growing in popularity, phishing and skimming attacks involving identity thefts by stealing confidential and personal information of customers has the potential to reduce confidence first and foremost in the financial sector.

The rise of an international criminal economy on the Internet with its tentacles in a variety of areas and with close linkages to a hacking community for which it provides the monetary resources and direction insofar as the kind of malware to be created and the networks to be penetrated goes, is a key component of the cyber threat. Whilst this would remain at the level of criminal activity, it has acquired dangerous proportions and impinges on national security when a state-criminal network-hacker nexus builds up. There is enough circumstantial evidence to show that some states have turned a blind eye to cyber-space centred criminal and illegal activities, perceiving certain advantages to be had from building up such a capacity.

While governments and government agencies, from the military to the intelligence community, have always had the ability to carry out disruptive activities in cyberspace, they exercised a certain degree of forbearance even during a war, in view of the cascading effects of such actions.[9] However, there was no such forbearance for intelligence agencies tasked with extricating secrets, and given a considerably free hand to pursue their vocation. Cyberespionage took the form of not just state-on-

---

[9] In 2003, the US intelligence agencies had drawn up plans for a cyberattack to freeze Iraq's financial system, but the Bush Administration, concerned about the possibility of a ripple effect leading to worldwide financial havoc, refused to give the go-ahead.

"Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk", *New York Times,* August 1, 2009, at http://www.nytimes.com/2009/08/02/us/politics/02cyber.html (Accessed September 22, 2012).

state spying but also the ex-filtration of intellectual property. China was condemned as behaving particularly egregiously, in terms of vacuuming intellectual property and military secrets from around the world. Though the US Government was at the forefront of these accusations, the initial revelations by Edward Snowden, an employee of a National Security Agency (NSA) sub-contractor, that the US was itself carrying out similar activities, has eroded much of the credibility of the US. This has been further compounded by subsequent revelations that the US has also conducted several offensive actions in cyberspace.[10]

The rising cost of waging physical wars and the disproportionately cost-effective ability to cause turbulence through actions in cyberspace has led peer competitors to skirmish in cyberspace.[11] As more states acquire cyber capabilities, the scope for instability increases exponentially. States have the same advantages in undertaking actions in cyberspace as the criminal networks. These include: the ease of expanding geographic reach to cover virtually the entire world at negligible cost, the difficulties of attribution, the concomitant advantage of deniability making it difficult for the target state to frame a suitable response and the increasing number of "e-ready" targets. This has given rise to the so-called Advanced Persistent Threats (APTs), primarily the handiwork of nation states. Only states can provide both the manpower and the financial power necessary for APTs to be both advanced and persistent. An average APT campaign would require manpower ranging from hackers to engineers, linguists and intelligence operatives.[12]

The targets that could have the greatest impact are those classified as critical infrastructure. Cyberspace has become the primary conduit for

---

[10] "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show", *Washington Post*, August 31, 2013, at http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html (Accessed November 1, 2013).

[11] According to one estimate, cyberattacks work out to about 4 cents per computer.

"Before the Gunfire, Cyber Attacks", *New York Times,* August 12, 2008.

[12] Dr. Kenneth Geer, "Highlights and Analysis on FireEye's Advanced Threat Report 2013", 19 March 2014, at https://www.brighttalk.com/webcast/7451/104453 (Accessed May 02, 2014).

financial transactions, and any successful attempt at large scale disruption could lead to financial chaos.[13] Other sectors that are targeted include the high-tech, energy, telecom and other government sectors. Think tanks have also been targeted as a means of watering-hole attacks: for example, their websites are compromised with malicious software that download onto the computers of visitors.[14]

## Perspectives on Cyberspace

Cyberspace is a phenomenon that has acquired a certain strategic position by virtue of global reach and its rapid integration into the global social, political and economic discourse and framework. At the same time, it is too nascent a medium to have regulatory norms and conventions in place.

The development of cyberspace worldwide has been informed by various factors and imperatives. However, the rapidity at which cyberspace has developed has meant that there are many different perspectives/imperatives at play simultaneously, resulting in widely varying approaches to cybersecurity.

### *The Engineering Perspective*

The Internet was developed in the academia by engineers who were mainly interested in problem-solving, and the same innovations and principles inform the functioning of cyberspace even today. Ad hoc workshops and task forces were created on the fly to grapple with problems as they arose, and decision-making was on the basis of rough consensus. Most of the innovations were freely available, which ensured that only the most feasible and adaptable of the several competing technologies survived, and these were quickly adopted. This approach has been romanticised as a model that worked perfectly till national

---

[13] As Michael McConnell, former Director of National Intelligence noted in his recent testimony before Congress, "While the US total GDP was just over $14 trillion [in 2009], two banks in New York move over $7 trillion per day in transactions."

Michael McConnell, "Seizing Opportunity While Managing Risk in the Digital Age", Testimony to Congress before the Committee on Commerce, Science and Transportation, February 24, 2010.

[14] *FireEye Advanced Threat Report: 2013,* Fireeye, Inc. February 1, 2014, at http://www2.fireeye.com/advanced-threat-report-2013.html (Accessed March 1, 2014).

governments stepped in and complicated matters by quarrelling over sovereignty and the like. However, the fact remains that cyberspace has become too big and too complicated to be run this way.[15] Engineers cannot be expected to address cultural and political issues that are now part of the discourse on cyberspace. However, the models of co-operation could be adapted and used on a wider scale.

## *The Information and Communications Technology (ICT) Perspective*

The ICT perspective evolved from an analysis of the impact of information technology on developed countries, in terms of its productivity and scope for innovation.[16] While the developed countries themselves (with the exception of Asian countries such as Japan and South Korea) did not consciously take the lead in harnessing information technology for the purpose of national development, letting the vagaries of the market dictate the direction, there arose a strong argument within developing countries for directed development of ICT. This was to be achieved through the use of ICT, which became an integral part of many national development plans.[17]

At the international level, such a perspective acquired an ideological hue with many non-governmental organisations taking the position that the developed countries were establishing their dominance over information networks under the garb of private sector-led initiatives and freedom of expression.[18] Though various attempts have been made by the United Nations (UN), beginning with the convening of successive World Summits on the Information Society in 2003 and 2005, the goal of bridging the digital divide and restructuring Internet

---

15 "IETF vs. ITU: Internet Standards Face-off", *Network World*, December 3, 2012, at http://www.networkworld.com/news/2012/120312-argument-ietf-itu-264594.html.

16 Sumit Roy, *Globalisation, ICT and Developing Nations: Challenges in the Information Age,* Sage Publications, Delhi, 2005, p. 115.

17 Peter Lovelock, "The Asian NII Experience", Paper presented at The Seventh Annual Conference of the Internet Society, Kuala Lumpur, Malaysia, June 27, 1997, at http://www.isoc.org/inet97/proceedings/E3/E3_2.HTM (Accessed December 11, 2012).

18 Parminder Jeet Singh, "Hyping One Threat to Hide Another", *The Hindu,* November 28, 2012, at http://www.thehindu.com/opinion/lead/hyping-one-threat-to-hide-another/article4140922.ece.

governance to reflect the international character of cyberspace was largely overlooked. The fragmentation among the developing countries and their susceptibility to pressure has seen many initiatives fall by the wayside since the developed countries and their multilateral organisations such as the Organisation for Economic Cooperation and Development (OECD) and the Organisation for Security and Cooperation in Europe (OSCE) have the resources and capabilities to undertake policy research and drive Internet policy.

## *The Private Sector Perspective*

Private companies were among the early adopters of cyberspace for the advantages it offered in terms of cost savings and efficiency. They had to contend with the many issues arising from the use of cyber networks, including the security of data and confidential and proprietary information; interestingly, a whole new industry of information security grew around this. In the US, where companies leveraged the information technology revolution of the 90s to reduce costs and increase efficiencies by outsourcing, information security came to be enforced by a combination of measures such as Payment Card Industry Data Security Standard (PCI DSS) and laws such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Government agencies such as the US National Institute of Standards and Technology (NIST) also set standards. At the international level, bodies such as the International Organisation for Standardisation (ISO), which is a consortium of the national standards institutes of 157 countries, established information security parameters such as the ISO 15443, ISO 31000 (Risk Management) and the ISO 22301 (Business Continuity Management).[19]

At the operational level, the primary focus of information security professionals has been to ensure the confidentiality, integrity and availability of data through processes, such as the 3R model for survivability, which focuses on resistance (ability to repel attacks); recognition (ability to detect and react to an attack) and recovery (keeping essential services going, during an attack, and restoring full service in

---

[19] *Information Technology - Security Techniques - A Framework for IT Security Assurance,* International Standards Organisation, at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=39733 (Accessed May 8, 2013).

the shortest time, after an attack).[20] This model has been held partly responsible for the lack of interest on the part of information security professionals to identify the source and perpetrators of an attack. There have been calls to add forensics to the model so that the perpetrators can be prosecuted on the basis of legally admissible evidence.[21]

Given the increasingly sophisticated cyberattacks, the moot question is whether the models that have been developed and adopted worldwide are adequate to deal with the escalating threats on enterprises in cyberspace. While more critical areas such as banking and finance have their own additional standards and rules, the challenge lies in their effective implementation.

## *The Law Enforcement Perspective*

In many countries, cyberspace governance defaulted to a law enforcement perspective because most of the issues that arose were related to cybercrime. Individuals have been at risk from the early days of cyberspace, but the sporadic nature of the initial crimes and their targets suggested that they were largely the handiwork of hackers and low-level criminal elements. Since then, cyberspace has seen a sharp rise in crimes like phishing, identity theft, online frauds using social networking sites, the disruption of critical information infrastructure by the use of botnets and cyberterrorism. The reason for this sharp rise has been ascribed to the lack of adequate legislation both at the national and international level; moreover, where such legislation exists, the lack of harmonisation in such laws has enabled cybercriminals to escape prosecution for crimes committed across various jurisdictions. While it is widely accepted that cybercrime can only be effectively combated by a real time response, the only existing avenues for international cooperation are the Interpol and Mutual Legal Assistance

---

[20] *The Survivable Network Analysis Method: Assessing Survivability of Critical Systems*, CERT Coordination Centre, Presentation: Software Engineering Institute, Carnegie Mellon University, Pittsburgh, at www.cert.org/archive/pdf/sna-short.pdf (Accessed November 15, 2013).

[21] B. Endicott-Popovsky and D. Frincke, "Adding the Fourth 'R': A Systems Approach to Solving the Hacker's Arms Race", in Proceedings of Hawaii International Conference on System Sciences (HICSS) 2006, 39 Symposium: Skilled Human-intelligent Agent Performance: Measurement, Application and Symposium at Kauai, at http://www.itl.nist.gov/iaui/vvrg/hicss39/4_r_s_rev_3HICSS2006.doc (Accessed February 18, 2012).

Treaties (MLATs). But MLATs are scarcely sufficient to combat cybercrimes in the 21st century, a fact brought out in the report of the Review Group on Intelligence and Communications Technology set up by President Obama following the furore after the Snowden revelations. The Committee noted that MLAT process has an average response time of 10 months, and suggested steps to speed up the process including, a) creating an online submission form for MLATs, b) streamlining the number of steps in the process, and c) streamlining provision of the records back to the foreign country.[22] With the top internet services companies still located in the United States, streamlining the law enforcement cooperation process in the United States would go a long way in combating international cybercrime activities.

That said, the countries whose law enforcement agencies have been working proactively against cybercrimes by augmenting their enforcement techniques and practices and adapting existing laws to tackle cybercrimes, etc. have had higher levels of success in managing cybercrime. They have also had a head start in the arduous process of building up case law in this new domain, also setting precedence for other judicial systems to follow.

The most widely known and possibly the only working transnational agreement that addresses criminal activity in cyberspace is the Council of Europe's Convention on Cybercrime. Adopted in 2004, the convention is a comprehensive document that lays down the rights and obligations of states for cooperating on cybercrime. Though it has been signed by many European states, Russia has been a notable exception. Non-European states that have signed the Convention include Canada, the US and South Africa. Japan is the only country in Asia to have acceded to the Convention. Other countries, including India, have been repeatedly pressed to join the Convention.[23] Russia's

---

22 The White House, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 12 December 2013 at www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Accessed January 10, 2013)

23 "India Asked to Join Convention on Cyber Crime"*, Outlook*, March 30, 2009, at http://news.outlookindia.com/item.aspx?657030 (Accessed March 1, 2012).

reservations centre on Article 32 of the Treaty which states:

> A Party may, without the authorisation of another Party:
>
> a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.[24]

Its concerns, which are shared by other countries including India, pertain to the implicit dilution of sovereignty inherent in these clauses. There have been many criticisms of the treaty, including that it is biased in favour of the law enforcement agencies without taking the rights of other stakeholders into consideration. While it has sweeping powers of computer search and seizure and government surveillance of voice, e-mail and data communications, there are no correspondingly detailed standards to protect privacy and limit the use of such powers by governments.[25] Some have also argued that the Convention is largely symbolic, and its long-term effectiveness is in doubt.[26]

## *The National Security Perspective*

Some countries have evolved a more comprehensive and holistic perspective on the threats posed by the unfettered flow of content and information to national security. Inasmuch as the monopoly over violence defined the supremacy of the state in an earlier era, the control over the use of technologies that facilitate the flow of information has become the primary focus of these states. As a case in point, the early

---

[24] Convention on Cybercrime, Council of Europe, at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (Accessed August 1, 2012)

[25] Greg Taylor, "The Council of Europe Cybercrime Convention: A civil liberties perspective", Electronic Frontiers Australia, at https://www.efa.org.au/Publish/coe_paper.html (Accessed May 8, 2013).

[26] Nancy E. Marion, "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation", *International Journal of Cyber Criminology,* 4 (1&2), January-July 2010 / July-December 2010, pp. 699-712.

Chinese focus on maintaining control over the Internet is believed to have emerged from its observation of the impact of loosening of the restrictions on information after the break-up of the Soviet Union as well as the role played by "facsimile machines, tape recorders, and Internet news groups" during the Tiananmen Square demonstrations.[27] Accordingly, the Chinese and the Russians have emphasised information security—rather than cyber security—on the premise that not just the networks but the information flowing through the networks can also threaten national security, and therefore, the state is within its rights to regulate both networks and content.[28] While this has been seen as being antithetical to democratic principles, since it amounts to censorship, the revelations of the all-pervasive scrutiny of metadata by the US NSA as well as other intelligence agencies in Western democracies has considerably weakened the very foundations of their opposition to the more intrusive strategies adopted by more authoritarian regimes in the name of national security.

## Cyberspace Governance: Outline of Cyberspace Governance Bodies

At the global level, cyberspace could be said to be very loosely regulated in that there is no overarching, centralised body with regulatory powers conferred on it. While this has not impeded the growth of cyberspace, and in fact has had the opposite effect, governance and regulation are a *sine qua non* for the effective functioning of any domain, virtual or real.

Nevertheless, currently, international collaboration on cyberspace takes place across four tracks: the technical track, the UN track, the regional track and the multilateral track. In addition, there are bilateral tracks

---

[27] Larry Press, William A. Foster and Seymour E. Goodman, *The Internet in India and China*, Annual Conference of the Internet Society, San Jose, California, 1999, at http://www.isoc.org/inet99/proceedings/3a/3a_3.htm (Accessed July 23, 2009).

[28] Tang Lan, "China's Perspective", in Ashley J.Tellis and Sean Mirski (eds.), *Crux of Asia: China, India and the Emerging Global Order,* Carnegie Endowment for International Peace, New York 2013, p. 187. Also see: UN Press Release, "Unregulated Information Highway Is Non-Traditional Security Threat With Too Many 'Traffic Accidents', China Tells First Committee, Warning Of Security Breaches", Sixty-sixth General Assembly First Committee 17th Meeting, October 20, 2011, at http://www.un.org/News/Press/docs/2011/gadis3442.doc.htm (Accessed August 23, 2012).

between like-minded countries to rationalise and coordinate their positions on cyberspace-related issues. A number of organisations have spearheaded discussions within these tracks.

## The Technical Track

### *Internet Engineering Task Force (IETF)*

The first institutional forums for discussing the progress of the Internet were technical in nature. The IETF was set up in 1986 and charged with ensuring the reliability and integrity of protocols that maintain the seamless flow of data streams, such as the Domain Name System (DNS) protocol and the Internet Protocol (IP). Its members, among others, included network operators, academics, and representatives of government and industry. Though the IETF hosts triennial meetings, much of its work is conducted via e-mail. All decisions are taken by a rough consensus. The IETF is part of a quartet of organisations, the others being: the Internet Architecture Board, the Internet Research Task Force and the Internet Engineering Steering Group—all operating under the aegis of the parent body, the Internet Society, which was created in 1992 as a formal corporate entity as a support structure for these bodies.[29]

### *Institute of Electrical and Electronic Engineers (IEEE)*

Cyberspace-related activities are only one part of the responsibilities of the IEEE. Its main area of work is to set standards for wireless networking—for instance, it was responsible for developing the 802.11, which was universally adopted for enabling encryption and wireless networking.[30]

### *International Electro-technical Commission (IEC)*

IEC is in the business of standards development. Its membership is made up of representatives deputed by the national committees of over 70 nations, which are themselves made up of representatives

---

[29] The Internet Society, at http://www.internetsociety.org/who-we-are/related-and-partner-organisations/standards-organisations (Accessed October 12, 2012)

[30] The IEEE Standards Association, at https://standards.ieee.org/ (Accessed October 13, 2012).

from each country's public and private sectors. It has worked in conjunction with the International Standards Organisation (ISO), a similarly structured non-governmental organisation based in Geneva, to draw up the ISO 27001 security standards as per which organisations ranging from companies to government agencies certify that their information security management systems meet these standards. These standards, though, are being increasingly criticised for being too checklist oriented and insufficient to address emerging cybersecurity risks.[31]

### *Internet Corporation for Assigned Names and Numbers (ICANN)*

While the aforementioned bodies are purely technical bodies, ICANN has both technical and policy functions. It was established in 1998 by the US department of Commerce, which had hitherto been overseeing the technical management of the domain name system, chiefly the allocation of IP addresses and managing root servers.[32] Unlike the other organisations, ICANN has an independent annual revenue flow (amounting to $ 70 million in 2012) arising out of the sale of domain names.

The corporation is overseen by a board of directors, composed of 21 representatives, of which 15 are voting members and 6 non-voting liaisons.[33] There are also a number of supporting and advisory organisations, the most prominent of which is the Governmental Advisory Committee (GAC), consisting of 111 countries, with other entities as observers.[34] The decision-making process in ICANN is highly convoluted as a consequence of attempts to bring in stakeholders at various levels, on the whole making a seemingly transparent system highly opaque.

---

[31] International Electrotechnical Commission, at http://www.iec.ch/ (Accessed October 13, 2012).

[32] "ICANN and the Problem of Legitimacy", *Duke Law Journal*, 50 (187), 250 (2000), p. 215-219.

[33] "About the GAC", ICANN, Governmental Advisory Committee, at https://gacweb.icann.org/display/gacweb/About+The+GAC (Accessed October 15, 2012).

[34] Jonathan Weinberg, "Governments, Privatisation, and 'Privatization': ICANN and the GAC", *Michigan Telecommunications and Technology Law Review*, 12 (189), 2011, at http://www.mttlr.org/voleighteen/weinberg.pdf (Accessed November 15, 2012).

## The UN Track

The UN would seem to be the institution of choice to resolve various issues concerning effective Internet governance given its position as the apex comity of states, as well as a multitude of subsidiary bodies for areas ranging from culture to human rights and technology. The UN made an early start in this direction with the convening of the World Summit on the Information Society (WSIS) in 2003 and 2005. One of its outcomes was the constitution of a Working Group on Internet Governance (WGIG) headed by Nitin Desai, the former UN Under-Secretary-General for economic and social affairs. This group came up with four organisational models for Internet governance which ranged from largely maintaining the status quo to radical restructuring by the creation of a Global Internet Council (GIC) which "would take over the functions relating to international Internet governance performed by the Department of Commerce of the United States Government".[35] But even before these recommendations, the US had declared that it would continue to "maintain its historic role" in the development of the Internet through its control of the root servers.[36] In the event, the only two institutions that saw the light of day from the WGIG recommendations were the General Advisory Council to ICANN and the Internet Governance Forum (IGF).

### *Internet Governance Forum (IGF)*

IGF was established by the 2005 WSIS, which was held in Tunis. It authorised the UN Secretary-General to create a mechanism to enable multiple stakeholders to discuss Internet governance. Its mandate was renewed for a further five years in 2011 by a resolution of the UN General Assembly.[37] The IGF meetings are held annually, and while the problems of funding and authority have reduced its effectiveness and

---

35 *Report of the Working Group on Internet Governance*, United Nations, Geneva, 2005, at http://www.wgig.org/docs/WGIGREPORT.pdf (Accessed November 12, 2012).

36 *U.S. Principles on the Internet's Domain Name and Addressing System*, US government Department of Commerce, June 2005, at http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system (Accessed December 18, 2012).

37 Resolution Adopted by the General Assembly, United Nations, February 2, 2011, at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/141 (Accessed August 12, 2012).

made it more of a talking shop, it remains the premier forum for governments, private sector, civil society organisations and individuals to engage in open discussion.[38]

A Working Group on IGF Improvements established under the auspices of the UN Commission on Science and Technology for Development (CSTD) has been meeting periodically to find ways and means to improve the IGF process as per a resolution of the Economic and Social Council passed in July 2010.[39] While the Working Group takes a multi-stakeholder approach, the governments exercise greater influence and the cultural gap between the various stakeholders has resulted in the meetings getting bogged down in procedural discussions rather than substantive issues.[40]

### *International Telecommunications Union (ITU)*

ITU is a UN agency that has three major and specific roles: 1) setting technical standards, 2) allocating radio spectrum and 3) providing technical assistance for capacity building to developing countries. The members of the ITU are a mix of delegations from UN member states, apart from the more than 700 members from the private sector who have been admitted as members after a screening process.[41]

The ITU was tasked with organising the WSIS in 2003, and as per its mandate from the WCIS, the ITU, in 2007, set the Global Cybersecurity

---

[38] This criticism was addressed by Lynn St. Amour, President of the Internet Society, in her inaugural address at the Third Internet Governance Forum held at Hyderabad, India, in 2008. http://www.internetsociety.org/igf-2008-opening-address (Accessed May 13, 2013).

[39] Working Group on Improvements to the IGF, United Nations Conference on Trade and Development (UNCTAD), at http://www.unctad.info/en/CstdWG/ (Accessed August 10, 2012).

[40] See various reports on the proceedings of the CSTD WG.

"CSTD Meeting on IGF Fails to Take Off", March 25, 2011, at http://news.dot-nxt.com/2011/03/25/cstdwg-collapse. Also see: "The CSTD WG on IGF, Multi-Stakeholderism, and Short Deadlines", CircleID, March 22, 2011, at http://www.circleid.com/posts/20110322_cstd_wg_on_igf_multi_stakeholderism_and_short_deadlines (Accessed October 12, 2012).

[41] International Telecommunications Union, at http://www.itu.int/en/about/Pages/default.aspx (Accessed May 15, 2013).

Agenda (GCA) "as a framework for international cooperation to promote cyber security [*sic*] and enhance confidence and security in the information society". A High Level Expert Group (HLEG) consisting of nearly a 100 individuals from various stakeholder organisations was constituted under the auspices of the GCA. Its report, submitted in 2008, was replete with dissenting views and exemplified the difficulties of arriving at a consensus in such a controversial area.[42]

The ITU and the IGF represent the competing approaches towards Internet governance, with the former favouring a top-down approach led by governments, and the latter supporting a bottom-up approach in which governments are just one of the many stakeholders. That both approaches are flawed is evident from the collapse of the World Conference on International Telecommunications (WCIT) held in December in 2012, where a significant number of countries either refused or put their ratification of the resolutions on hold, because they perceived them as being the thin edge of the wedge for authoritarian countries to legitimise their attempts to control information flows over the Internet.

## *UN Group of Governmental Experts (UNGGE)*

The genesis of the UNGGE can be traced to a resolution introduced by Russia in 1998.[43] Russia had proposed the establishment of the GGE to examine the issue of information security, and the first group of governmental experts was set up in 2004 by the First Committee, one of the UN General Assembly's six committees, on Disarmament and International Security.[44] However, there was no consensus on the recommendations because of the divergent positions taken by Russia and China on the one hand and the US and its European allies on the

---

42 "ITU Gateway for WSIS", at http://www.itu.int/itu-wsis/ (Accessed May 15, 2013).

43 "Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations, at http://www.un.org/disarmament/topics/informationsecurity/ (Accessed May 15, 2013).

44 Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012", ICT for Peace, 2012, at http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.

other, on even the issues to be discussed by the GGE.[45] A second group, established in 2009, submitted its report in 2010 with a number of recommendations.[46]

The 2010 GGE Report recommended dialogue among states on the norms to address the collective risks and for protecting the critical national and international infrastructure. It also called for measures to promote confidence, stability and risk reduction. While the report was only stating the obvious, the GGE nonetheless offered governments an important forum to take cognisance of unfolding threats in cyberspace and for narrowing differences to the extent possible.[47] It is also an early experiment in whether existing principles of the UN Charter and international law can be applied in cyberspace. There is much that is achievable by way of cooperation, whether it be the exchange of best practices, the sharing of information, capacity building, rationalisation of procedures to speed up cybercrime investigation, etc., which can be regulated through this mechanism. A third group was established in 2011 to carry forward the work and recommendations of the 2010 report of the GGE. This group, like the earlier ones, consisted of five permanent members and 10 other member states.[48] It submitted its report in June 2013.[49] The two main agreements in the report were as follows: 1) Existing international law applies in cyberspace 2) Voluntary CBMs can play an important role in advancing peace and security

---

45 Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security", Belfer Centre for Science and International Affairs, Harvard Kennedy School, Cambridge, Mass., September 2011, p. 22.

46 Tikk-Ringas attributes the forward movement in this GGE, as compared to the earlier GGE, to a number of factors, including the Obama Administration's more cooperative approach. Eneken Tikk-Ringas, No. 45, p. 7.

47 See the press release of the US State Department following the conclusion of the third GGE which reports considerable progress in narrowing differences:

"Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues", US Department of State, June 7, 2013, at http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm (Accessed July 12, 2013).

48 Other than the permanent members, the other states included Argentina, Australia, Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia and Japan. India has been a member of all three GGEs dealing with this issue.

49 http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (Accessed November 15, 2013).

While the efforts of the GGE have been lauded by some[50], there are others who see these as being ill-suited for cyberspace. In the words of Jonathan Zittran:

> Such efforts import from professional diplomacy the notion of process and unanimity above all. Their solution for the diffculties of individual state enforcement on the Net is a kind of negotiated intellectual harmony among participants at a self-conscious summit - complex regimes to be mapped out in a dialogue taking place at an endlessly long table, with a role for all to play. Such dialogues end either in bland consensus pronouncements or in final documents that are agreed upon only because the range of participants has been narrowed.[51]

Nevertheless, the GGEs have a better track record of producing results compared to other fora, and could provide the outlines for a viable mechanism for norm making in cyberspace. The main drawback to the GGE process is the turnover in the participating countries in each successive GGE.

## The Regional Track

Most of the regional tracks have grown out of the multilateral forums, which exist across continents.

### *Asia*

Within Asia, much of the discussion has been perfunctory with the emphasis largely on cybercrime-related issues. Even as most of the major cyber attacks have taken place in West Asia, the few multilateral organisations where meaningful discussion on cyber issues is taking place are largely in the East.

### Association of South East Asian Nations (ASEAN)

ASEAN has been actively promoting the concept of cybersecurity among its member states with the active participation and support of

---

[50] Tim Maurer, No. 45, p. 50.

[51] Jonathan L. Zittrain, *The Future of the Internet — And How to Stop It,* Yale University Press, New Haven & Penguin, UK, 2008, pp. 242-243.

the US. Cybercrime was placed on the agenda of the ASEAN ministerial meetings as early as 2001.[52] Its 2009-2015 *Roadmap for an ASEAN Community* focuses on cybercrime, but a unified stand would give it an influential voice in cybersecurity discussions. ASEAN, in the course of its history has spawned a number of ancillary organisations such as the ASEAN Regional Forum (ARF) and the Council for Security Cooperation in the Asia Pacific (CSCAP) that also have cybersecurity on their agenda.

## ASEAN Regional Forum (ARF)

ARF is a larger body consisting of 27 countries including the 10 ASEAN member states (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam); the 10 ASEAN dialogue partners (Australia, Canada, China, the EU, India, Japan, New Zealand, ROK, Russia and the United States) as well as the Democratic People's Republic of Korea (DPRK), Mongolia, Pakistan, Timor-Leste, Bangladesh and Sri Lanka.

The ARF organised a series of seminars on cyberterrorism between 2004 and 2007, but some member countries were uncomfortable with the notion of cyberterrorism.[53] The "Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space" was released at the end of the 13th ASEAN Regional Forum at Kuala Lumpur in 2006. It urged member countries to enact laws and adopt policy frameworks on cybercrime and cybersecurity.[54] In 2012, the ARF again kick-started its program on cybersecurity with the first workshop: "Workshop on Measures to Enhance Cyber Security - Legal and Cultural Aspects" being hosted by China in September 2013. In March 2014, a second workshop on Cyber Confidence Building Measures was held in Malaysia as part of a larger ARF Work Plan on

---

52 Ralf Emmers, *The Securitization of Transnational Crime in ASEAN*, Working Paper, Institute of Defence and Strategic Studies, Singapore 2002, p. 14

53 Rodolfo Severino, *The ASEAN Regional Forum*, Institute of Southeast Asian Studies, Singapore, 2009, p. 98

54 Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space of the thirteenth ASEAN Regional Forum, 2006, at http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html (Accessed May 20, 2013).

"Security of and in the Use of Information and Communications Technologies (ICTs)".

## Council for Security Cooperation in the Asia Pacific (CSCAP)

CSCAP, of which India is a member, deals with cybersecurity at the Asian regional level. The CSCAP working groups meet twice a year and make recommendations for consideration at the Track 1 level.[55] A working group on transnational crime had focused on cybercrime as early as 2001.[56] In 2004, the working groups were replaced by study groups. A study group on cybersecurity was created in 2009, and it published its report in 2011.[57]

## Asia-Pacific Economic Cooperation (APEC)

APEC is another organisation which has been deliberating on cybersecurity with active inputs from the US. APEC's Telecommunication and Information Working Group (TEL) has been tasked with coordinating cybersecurity activities for the organisation with special focus on incident response, developing information security guidelines, combating cybercrime and monitoring the security implications of emerging technologies as well as fostering international cooperation on cybersecurity.[58]

---

55 *Study Groups*, CSCAP, at http://www.cscap.org/index.php?page=study-groups (Accessed May 20, 2013).

56 Desmond Ball and Kwa Chong Guan, "Assessing Track 2 Diplomacy in the Asia-Pacific Region", *A CSCAP Reader,* 2010, p. 28.

57 "Ensuring a Safer Cyber Security Environment*", Memorandum No. 20*, May 2012, Council for Security Cooperation in the Asia Pacific (CSCAP), at http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%2020%20%20Ensuring%20a%20Safer%20 Cyber%20Security%20Environmenet.pdf (Accessed May 15, 2013).

58 "Promoting a Safe and Trusted ICT Environment", *Strategic Action Plan: 2010-2015*, APEC Telecommunications and Information Working Group, 2010, at http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2010_tel/ActionPlan.aspx (Accessed May 15, 2013).

## *Europe*

### Council of Europe

The Council of Europe (CoE), founded in 1949, has become an important stakeholder in cybersecurity discussions, by the creation and propagation of a Convention on Cyber Crime in 2001 which seeks to harmonise cybercrime-related legislations in various countries. Russia has been one of the notable opponents of the Budapest Convention despite being a member of the CoE, and has been particularly vociferous in its protests against Article 32, which calls for a softening of state sovereignty in the interests of fighting cybercrime.

### Organisation for Security and Co-operation in Europe (OSCE)

OSCE is one of the largest intergovernmental security organisations with 55 participating European states along with Canada and the US. While cybersecurity had been sporadically addressed in the OSCE, a working group was established in 2012 to 1) elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability and stability; 2) reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs and 3) help build consensus for the adoption of such a set of CBMs.[59]

After an eventful process which included hacking of an OSCE server and release of confidential documents by the hactivist group Anonymous, the OSCE passed the *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* in December 2013.[60]

---

[59] "Decision No. 1039 Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Organization for Security and Co-Operation in Europe, April 26, 2012, at http://www.delegfranceosce.org/IMG/pdf/pcdec1039_reduce_risk_of_conflicts_from_use_of_ICT.pdf (Accessed Nov. 28, 2013).

[60] "Permanent Council Decision No. 1106. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Dec. 3, 2013, at http://www.osce.org/pc/109168 (Accessed Jan. 08, 2014).

The following recommendations were included:

1) Exchange of information on national views on threats in the use of information and communications technologies

2) Exchange of information on measures being taken by states to ensure an open and reliable Internet

3) Exchange of information on strategies, policies and programs regarding cybersecurity

4) Consultations to reduce misunderstandings and misperceptions

5) Cooperation between state bodies responsible for establishing best practices

6) Exchange of information on national incident response policies and practices

7) Establishment of methods of rapid communication at senior policy levels regarding national security concerns

8) Exchange of information and dialogue on terms of reference used nationally in order to diminish misunderstandings.

Russia added an interpretative statement to the statement, noting that while supporting the decision, "the Russian Federation will be guided in its implementation by a firm commitment to the principles of non-interference in the internal affairs of States, their equality in the process of Internet governance and the sovereign right of States to Internet governance in their national information space, to international law and to the observance of fundamental human rights and freedoms."[61]

## Multinational Tracks

### *Organisation for Economic Cooperation and Development (OECD)*

OECD is a 34-member grouping consisting largely of high-income countries. As the name suggests, its primary focus is economic, but it has also been active in pushing forward its proposals in the security

[61] Ibid. p. 4.

and political arenas. The policy development process within the OECD is multilayered and consists of over 200 committees and working groups. The bodies dealing with cybersecurity include the Working Party on Information Security and Privacy (WPISP), Business and Industry Advisory Committee (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and Internet Technical Advisory Committee (ITAC). The Information, Computer and Communications Policy (ICCP) Committee is the apex committee.[62] India has observer status in the ICCP Committee and in some other subordinate working parties.[63]

OECD has brought out a large number of documents on issues related to cyberspace; it has largely pushed for status quo in Internet governance while strengthening punitive provisions relating to intellectual property. It has been accused of trying to push the agenda of the rich countries that benefit from the status quo.[64]

### *North Atlantic Treaty Organisation (NATO)*

NATO has been actively involved in working out the modalities of a military response to cyber attacks within the framework of the organisation, particularly in relation to Article Five which calls for collective defence. Considerable energies have been expended on setting up think tanks such as the Cooperative Cyber Defence Centre of Excellence (CCDCOE) to examine these issues, particularly in the legal realm.[65] Most recently, the Centre brought out the so-called *Tallinn*

---

[62] Committee for Information, Computer and Communications Policy (ICCP) has the following Working Parties reporting to it: Working Party Indicators for the Information Society (WPIIS), Working Party Communication Infrastructures and Services Policy (CISP), Working Party on Information Security and Privacy (WPISP) Working Party on the Information Economy (WPIE).

[63] "On-Line Guide to OECD Intergovernmental Activity", at http://webnet.oecd.org/OECDGROUPS/Bodies/ListByRoleView.aspx (Accessed January 03, 2013).

[64] Parminder Jeet Singh, "A Development Agenda for Internet Governance – Call for a 'Framework Convention on the Internet"', IT for Change Position paper, Delhi, July 2008, at http://thepublicvoice.org/events/seoul08/OECD-ITfC.pdf (Accessed December 15, 2013).

[65] Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", Issue Brief , Atlantic Council, 2012, at http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf Accessed on 1 February 2013

*Manual*, a brief on the applicability of the laws of armed conflict and other relevant international documents in cyberspace.[66]

## *Shanghai Cooperation Organisation (SCO)*

SCO was established in 2001; it comprises the countries of the Eurasian region and China and has been active in formulating and pushing policies on cybersecurity governmental experts on cybersecurity was established in 2006. An intergovernmental agreement among the SCO member states on cooperation in providing Information Security was signed in 2009 and came into effect in 2011 after ratification by six member states. The member states have taken united positions to push their proposals in international forums such as the UN.

## *IBSA*

The India, Brazil, South Africa (IBSA) grouping has been active in internet governance related issues with Brazil hosting a multistakeholder meeting on Internet Governance in 2011. India's proposal to create a Committee for Internet-Related Policies (CIRP) submitted to the United Nations in 2011 was largely based on the proceedings of this meeting.

## *BRICS*

The Brazil, Russia, India, China (BRICS) grouping has also had cybersecurity on their agenda with discussions being spearheaded by the respective National Security Advisors of these countries.[67] As with IBSA, the lack of a secretariat and differing objectives among the partner countries are the major obstacles to better co-ordinated strategies.

---

[66] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.

[67] Transcript of Media Briefing by National Security Advisor after BRICS Meeting of High Representatives on National Security, *Ministry of External Affairs, India,* January 10 2013 at http://www.mea.gov.in/media-briefings.htm?dtl/21046/Transcript+of+Media+Briefing+by+National+Security+Advisor+after+BRICS+Meeting+of+High

## Other Tracks

In addition to the aforementioned ones, there are a number of other functional tracks, notably for law enforcement and cybersecurity co-operation, such as the Interpol, Forum of Incident Response and Security Teams (FIRST) and Asia Pacific CERT (APCERT). While these have largely been involved in co-ordination, they are gradually becoming more pro-active. Interpol, for instance, has opened an Interpol Global Complex for Innovation (IGCI) in Singapore with a focus on cybercrimes. Its Europe-centric counterpart, EUROPOL also launched the European Cybercrime Centre (EC3) in January 2013.

Despite the plethora of organisations and technical and policy oriented frameworks, the rising tide of malicious activities are affecting governments, corporations and individuals. There is increasing demand from the private sector that they be allowed to respond to attacks more proactively, using the euphemism "Active Cyber Defence". From being a response considered on the fringes of information security, this approach has become mainstream in recent years.[68] The essence of active cyber defence is creating a legal framework in which technically feasible counter-measures could be legitimised.

[68] This topic was the main thememe at CYCON 2014, the annual conference of the NATO Centre of Excellence in Estonia in 2014.

*CHAPTER - III*

# India's Quest for Cybersecurity

Many commentaries refer to India as a cyber power,[69] something that might appear to be at odds with the reports regarding the vulnerabilities in India's cybersecurity. The Indian Government estimates that there are only 556 cybersecurity experts in the country.[70] But it goes without saying that India will have an influential role to play in cyberspace because of its demonstrated capacities and capabilities in information technology and the increasing number of its population migrating to cyberspace.[71]

India's inadequate cybersecurity posture might seem strange for a country that is seen as a software superpower. The reasons for this lie both in the history of cyberspace in India as well as the various perspectives that push and pull cybersecurity policies in various directions, and get reflected in India's international posture on cyberspace.

## Indian Cyberspace: A brief history

Even though the conventional wisdom is that outsourcing was the main driver of the development of information technology in India in the 90s, the National Informatics Centre was set up as early as 1975 with the goal of providing information technology solutions to the government.[72] The two other organisations established during that

---

[69] For instance, see Interview with John Mroz, President, East-West Institute, "India: An Emerging Cyber Power", East West Institute, September 24, 2012, at http://www.ewi.info/idea/india-emerging-cyber-power (Accessed December 18, 2012).

[70] "An IT Superpower, India Has Just 556 Cyber Security Experts", *The Hindu,* June 19, 2013, at http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece (Accessed June 20, 2013).

[71] "Shyam Saran, India and the Age of Acceleration", *The Tribune*, August 14, 2013, at http://www.mea.gov.in/articles-in-indian-media.htm?dtl/22073/India+and+the+Age+of+Acceleration (Accessed August 20, 2013).

[72] The National Informatics Centre now hosts some 30,000 government websites in addition to its other functions.

period were the Computer Maintenance Corporation (CMC Ltd.)[73] and the National Centre for Software Technology (NCST). While the CMC took over IBM India's maintenance operations in 1978, the NCST developed indigenous e-mail and networking software. An experimental 32 kbps packet switched Very Small Aperture Terminal (VSAT) network connecting Ahmedabad, Mumbai and Delhi was established in 1982. Based on these experiences, between 1986-88, the government commissioned three networks: INDONET, which connected the IBM mainframe installations that made up India's computer infrastructure; the National Informatics Centre Network (NICNET), a nationwide VSAT network for public sector organisations, which also connected the central government with the state governments and district administrations and the Education and Research Network (ERNET), which served the academic and research communities.[74] The first connection to the global Internet was established by the NCST in February 1989.[75]

The Videsh Sanchar Nigam Limited was set up in 1986 as a public sector undertaking to provide international communications. It became central to the development of the Internet in India following the outsourcing boom in the 1990s. Prime Minister Rajiv Gandhi brought in B.K. Synghal, a telecom professional from the US, to head the company in 1991. Though it was initially focussed on providing international connectivity to BPO companies, in 1994, the company was given the mandate of "connecting the common man", and it started providing internet connections to individuals, though at astronomical rates.[76] Internet service for the public was made available from August 14, 1995. Though there was heavy demand for the service,

---

[73] "CMC Ltd: We've Come a Long Way", n.d., at http://www.cmcltd.com/about_us/history.shtml (Accessed December 13, 2012).

[74] Peter Wolcott, "The Provision of Internet Services in India", in R.M. Davison, R.W. Harris, S. Qureshi, D.R. Vogel and G.J. de Vreede (eds.), *Information Systems in Developing Countries: Theory and Practice*, University of Hong Kong Press, Hong Kong, 2005, p. 256, at http://mosaic.unomaha.edu/India_2005.pdf (Accessed March 15, 2009).

[75] Peter Wolcott and Seymour E. Goodman, "Global Diffusion of the Internet - I: India: Is the Elephant Learning to Dance?", *Communications of the Association for Information Systems*, 11 (32), 2003, at http://aisel.aisnet.org/cais/vol11/iss1/32, p.571 (Accessed June 15, 2009).

[76] A 128 kbps dial-up connection was available for ' 15,000.

it was constrained by a number of factors including the slow expansion of the network of gateway servers; reduced bandwidth to the US where most of the content was located and the government's reluctance to change VSNL's monopoly status because it did not want to lose control over this new medium of communication.[77] In 1995, there was a partial lifting of the monopoly, with 10 companies being allowed to provide e-mail services though they had to pay very heavy annual licence fees. Subsequently, the New Internet Policy of 1998, allowed private Internet Service Providers (ISPs), but they were to connect to the Internet only through the VSNL gateway "in deference to the bogey of security, pornography and subversive information 'invading' India over the Internet".[78] According to the policy, ISPs did not have to pay any licence fee for the first five years and were also allowed to have 49 per cent foreign equity investment. The first private ISP, Satyam Infoway, began operations in 1997.[79] The entry of private ISPs saw the Internet user base grow from less than a million in 1999 to over 15 million by 2003.[80] Another factor responsible for its spread was the entry of several companies, funded by venture capitalists, which catered to the content and e-commerce space, on the model of similar companies in the US and elsewhere. The first of these was Rediff which began operations in 1995. Many of these companies were impacted by the bursting of the dot-com bubble in 2001.

As early as 1998, the government of the day had set up a National Task Force on Information Technology and Software Development which in its report and recommendations implicitly recognised the fact that becoming an information technology power house did not rest on one or two policy decisions, but a series of enablers that provided the conditions necessary for a whole ecosystem to flourish.

---

77 The only other entity allowed to have its own gateway was the Software Technology Parks of India (STPI), an organisation set up in 1991 to facilitate software exports.

78 T H. Chowdary, "The Internet Divide", *Telecommunications*, September 1, 1997, HighBeam Research, at http://www.highbeam.com/doc/1P3-14693541.html (Accessed November 16, 2012)

79 "VSNL Braces for Competition from Private ISPs", *India Abroad,* 1998, HighBeam Research, at http://www.highbeam.com/doc/1P1-22128808.html (Accessed June 15, 2012).

80 Ibid.

Among the terms of the reference of the Task Force relevant to cyberspace were the following:

1. Recommend a strategy for the extensive use of Information Technology in all areas of national economy - agriculture, industry, trade and services - as a critical input in making India a global economic power.
2. Prepare the design for building a world-class physical, institutional and regulatory IT infrastructure, which is appropriate for India.
5. Suggest measures for achieving a massive expansion in the use of the Internet by all sections of society, especially in business and education, and development of Indian content on the Internet.
6. Recommend a strategy for boosting the learning and use of Information Technology in Indian languages.
11. Devise a strategy for establishing a strong and internationally competitive domestic manufacturing base for computers, computer components and peripherals.
13. Suggest an appropriate legal frame work for the creation of an IT-based society, with due focus on Intellectual Property Rights (IPR), secrecy, security and safety of information.
14. Recommend how India can leverage its global competitiveness in InfoTech to play a prominent role in the development of IT in other countries, especially those that are underdeveloped.

The Committee set a number of goals and made 108 recommendations to achieve those goals. Sixteen years on, it is instructive to revisit them both in order to see the extent to which those goals have been achieved, and whether any of those recommendations, particularly to do with cyberspace are worth resuscitating.

The first goal was to "accelerate the drive for setting up a world class Info Infrastructure with an extensive spread of Fibre Optic Networks, Satcom Networks and Wireless Networks for seamlessly interconnecting the Local Informatics Infrastructure (LII), National Informatics Infrastructure (NII) and the Global Informatics Infrastructure (GII) to ensure a fast nation-wide onset of the INTERNET, EXTRANETs and INTRANETs." The specific target was to achieve a 30 per cent of annual growth rate from the 1998 level

of Fibre Optic backbone of 75,000 route kilometres, VSATs of aggregate capacity of over 300 Megabit Per Second, Satellite Transponders of aggregate capacity of more than 3000 Megahertz, etc.

The second goal was for "creating a congenial ambience for exporters of IT Software and IT Services (including IT-enabled services) to reach the export target of US $ 50 billion by the year 2008".

The third goal was for "IT for all by 2008". Recognising Information Technology to be a frontier area of knowledge, and also a critical enabling tool for assimilating, processing and productivising all other spheres of knowledge, the Task Force suggested a national campaign to universalise computer literacy and also to spread the use of computers and IT in education.

A fourth goal was to enable "IT in government". This contained recommendations of direct relevance to cybersecurity:

101. An Information Security Agency shall be set up at the National level to play the role of Cyber Cop.

102. A National Policy on Information Security, Privacy and Data Protection Act for handling of computerized [*sic*] data shall be framed by the Government within six months.

104. The cryptology and Cyber Security knowledge and experience developed by the defence establishments shall be suitably transferred to the civilian information security agencies for wider dissemination in the country to increase information security, network security and bring about a greater degree of secure use of EFT, digital signature, etc.[81]

The moot point is that all four goals suggested by the task force would have had to be pursued with the same amount of vigour for the eco system to be built up. Sixteen years on, the government has only begun to implement many of these recommendations. Broadband penetration stands at about 10 per cent of the population, with much of it concentrated in urban areas. Recognising the need for expansion, the government is implementing a National Optical Fibre Network

[81] Y. Deva, *Secure Or Perish*, Ocean Books, Delhi, 2001, p. 53-54.

(NOFN) Plan which aims to add another 500,000 route kilometres of optical fibre to the 670,000 route kilometres which are already available with public sector companies such as the Bharat Sanchar Nigam Ltd. (BSNL), Railtel Corporation of India Ltd. and Power Grid Corporation. On the flip side, as connectivity expands and grows, the vulnerabilities inherent in the networks also grow (see Figure 1).

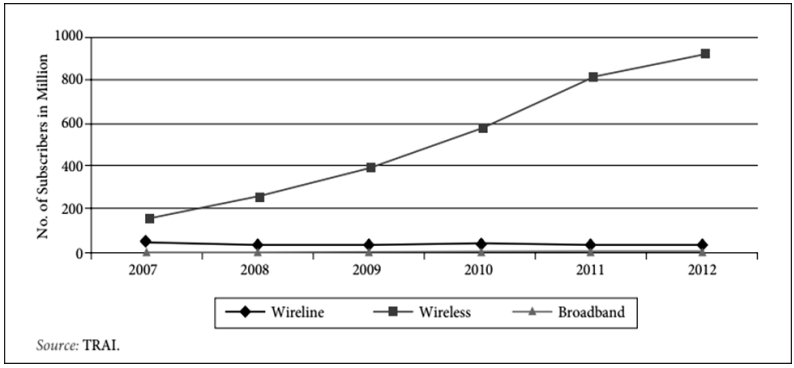



Figure 1. Number of Telephone, Mobile and Broadband Connections 2007-2012[82]

The sudden rise in telephone density was partly the outcome of the First National Telecom Policy of 1994, which had elements of an ICT strategy incorporated in it.[83] This rise paled in comparison with the increase in the number of mobile phones that was fuelled by subsequent telecom policies.[84] Aggressive competition in the mobile wireless space led to explosive growth in this segment, with mobile subscriptions reaching almost 800 million while fixed telephone lines languished at 50 million. With broadband, till recently, largely available through wire line subscription, the broadband Internet subscriber base also remained consistent at around 10 per cent of the population. This population is gradually increasing with the arrival of 3G and 4G broadband wireless technologies as also a renewed effort on the part of the government

---

82 "Economic Sectors", *Draft 12th Five Year Plan*, *2012-2017*, Planning Commission, 2, 2012, p. 260.

83 *National Telecom Policy 1994*, Department of Telecommunications, Government of India.

84 *National Telecom Policy 1999 and 2012*, Department of Telecommunications, Government of India.

to expand the broadband network through initiatives such as the National Knowledge Network (NKN) and the NOFN.[85] These programs aim to bring broadband to 2.5 lakh villages, 400,000 public internet access points, and WIFI in 2.5 lakh schools and universities.

## *Approaches to Cyberspace in India*

Two main approaches have impacted cyberspace. The first is the realist approach which places the state at the centre of international politics and enjoins upon it to do whatever necessary to secure a place at the high table on international cyber policymaking. This approach also accords priority to developing capabilities, and has little faith in the ability of states to arrive at a consensus on, what is essentially, an anarchic space. Since states are the primary actors, it is their responsibility to develop defensive and offensive cyber capabilities to secure their survival.[86] According to Mary McEvoy Manjikian, in the case of the US:

> From the outset, two different narratives have existed to describe cyberspace - its essence, its utility, and its relation to issues of state power. The stories differ in their basic assumptions, the terms they use, and their views of cyberspace's development. For the last 30 or so years, both stories have coexisted in a tense relationship with one story achieving prominence over the other at key junctures, usually as the result of historical events such as the 1991 Persian Gulf War or the terrorist attacks of September 11, 2001. The Internet's technical developers and their fellow academics tell a neoliberal story while the military and strategic studies community tells a neorealist story. Both stories acknowledge cyberspace as a new type of territory, with unique challenges as well as advantages for participants. [87]

---

[85] The NKN is a high speed network that connects educational institutions, while the NOFN plans to take broadband right down to the panchayat level. More details may be found on the respective websites: http://www.nkn.in and http://www.bbnl.nic.in/.

[86] Raja Mohan, "Cyber War: Blaming Pakistan Is Not Enough", *Indian Express*, August 20, 2012, at http://www.indianexpress.com/news/cyber-war-blaming-pakistan-is-not-enough/990637 (Accessed November 27, 2012).

[87] Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonising of the Internet and the extension of Realpolitik", *International Studies Quarterly,* 54 (2), June 2, 2010, pp. 382-383.

In India, though the realist approach is yet to be fleshed out in military doctrines, it has found place in grand strategy formulations such as *Nonalignment 2.0: A Foreign and Strategic Policy for India in the Twenty-first Century*.

Much of the internal debate on cyberspace though takes place at the liberal end of the spectrum and revolves around issues of open and equitable access, freedom of speech and expression and privacy. Since all these are increasingly tied up with security in cyberspace and issues of surveillance, they also impact cybersecurity issues. Both approaches look on the concept of the global commons as being the golden mean though the points of departure are vastly different. Both accepted that cyberspace is a "global commons" akin to air, sea and space, "which no one state may own or control, and which is central to life as we know it today".[88] However, while some saw this in terms of universalisation of values; others saw it as a way of both sharing responsibility and preventing the domination of cyberspace by any one country. As a global public good, it is seen to be both the right and responsibility of states to adhere to the stated goals of keeping the commons "open, global and secure".

The global commons concept has found resonance, most recently, in Japan's cybersecurity doctrine.[89] Even as it has been mentioned as a joint goal in India-US communiqués[90] as well as research articles[91], it

---

88 Shiv Shankar Menon, Speech, at the Shangri La Dialogue, June 05, 2010, at http://www.iiss.org/conferences/the-shangri-la-dialogue/shangri-la-dialogue-2010/plenary-session-speeches/second-plenary-session/shivshankar-menon/ (Accessed October 10, 2012).

89 *Towards Stable and Effective Use of Cyberspace,* Ministry of Defence, Japan, September 2012, p. 2, at http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf (Accessed October 12, 2012).

90 For instance, in the context of India-US relations, managing the security of the global commons was identified as one of the chief areas of cooperation for the two countries in the joint statement issued at the end of the Obama visit. The operative sentence read, "In an increasingly inter-dependent world, the stability of, and access to, the air, sea, space, and cyberspace domains is vital for the security and economic prosperity of nations. Acknowledging their commitment to openness and responsible international conduct, and on the basis of their shared values, India and the United States [will] explore ways to work together, as well as with other countries, to develop a shared vision for these critical domains to promote peace, security and development."

91 C. R. Mohan, "Rising India: Partner in Shaping the Global Commons"*? The Washington Quarterly,* 33 (3), pp. 133–148.

lost cachet in the US[92] and amongst other cyber powers for a variety of reasons. Firstly, there is a perception that this is resulting in the so-called tragedy of the commons, with none of the stakeholders being willing or able to take responsibility for the security of cyberspace, various actors are taking advantage of the lacunae to unleash malicious attacks.[93] Secondly, there are doubts whether the very concept of global commons applies to cyberspace since it is composed of networks and structures that are owned by various corporations and governments. Thirdly, many governments are uneasy about the complete lack of control over cyberspace, and have made determined efforts to assert authority, at least within their sovereign territories. They have also sought to claim legitimacy for their actions by pushing these alternative approaches at a variety of multilateral forums.

## Perspectives and Imperatives Impacting Cybersecurity

While there is a clearly discernible ICT perspective, which has had an impact on the development of cyberspace, the law enforcement/ national security imperatives are acquiring primacy, but with an inward rather than an outward focus, even though the threats are primarily external.

## The Private Sector Perspective

As seen above, outsourcing has been a major factor in the spread of cyberspace since these communication networks were essential for the industry. The "National Task Force on IT and Software Development" set up in 1998 was largely composed of the senior executives of private companies along with bureaucrats, and a sprinkling of military officers, academics and policymakers. Of the 108 recommendations made by

---

92 The US National Military Strategy of 2004 refers to the global commons of air, seas, space and cyberspace, whereas the US National Military Strategy published in 2011 distinguishes between the global commons and the "globally connected domains" such as cyberspace.

*The National Military Strategy of the United States of America,* 2011, Department of Defence, p.3. Also see: James A. Lewis, "Cybersecurity: Next Steps to Protect Critical Infrastructure", Testimony to the US Senate Commerce Committee, February 23, 2010.

93 *NATO in the Cyber Commons*, NATO Allied Command Transformation Workshop, Tallinn, Estonia, October 19, 2010.

the Task Force, 50 were for business, 23 for infrastructure and the rest for development.

Despite these inputs, the Information Technology Act of 2000 largely dealt with only those aspects of information technology that were relevant to outsourcing with neither cybersecurity nor cybercrime, as terms, appearing anywhere in the legislation.[94] The Preamble to the Act stated that it was an act "to provide legal recognition for transactions carried out by means of electronic date interchange and other means of electronic communication, commonly referred to as 'electronic commerce"'.

Even the amendments made in 2006, largely added provisions related to outsourcing and indemnifying Internet services against certain liabilities.[95] The proposed amendments in 2006 were prompted by the arrest of the CEO of an online marketing site in 2004 because the site was used to peddle pornographic material. The resultant outcry led to the constitution of a committee in 2005 to examine the Act and suggest how it could be improved in line with other such Acts in place around the world.[96] In the event, these amendments were not passed, as they were seen to be too industry-friendly.

It may be seen that the private sector is both a leading provider and user of cyberspace, and thus has a major influence on cybersecurity policies. Companies that use cyberspace to facilitate their commercial activities are focussed on ensuring that government policies do not add to their costs or come in the way of their doing business. For instance, in banking, there is a strong regulatory body in the form of

---

94 *Information Technology Act, 2000*. Government of India, at www.dot.gov.in/Acts/itbill2000.pdf (Accessed August 15, 2012).

95 The Bill was listed for business in the Rajya Sabha as follows: "To incorporate the recent developments nationally and internationally particularly with reference to provisions related to data protection and privacy in the context of Business Process Outsourcing (BPO) operations, liabilities of network service providers, computer related offences, regulation of cyber cafes, issues relating to child pornography, etc." Available at http://164.100.24.167/newsite/lb/legislative/bil/billexpected206.htm (Accessed February 23, 2012).

96 A. Balakrishnan, *The Wave Rider: A chronicle of the Information Age*, Pan Macmillan, Delhi, 2012, p. 72.

the Reserve Bank of India (RBI); however, in many cases, banks have only paid lip service to the diktats of the RBI.

More active lobbying activities are carried out by both multinational and Indian companies who utilise cyberspace for their core commercial activities. These range from Indian outsourcing companies to multinationals such as Google and Facebook that have a huge stake in one of the fastest growing internet subscriber bases in the world.

## The ICT Perspective

The ICT perspective has also been an important factor in India's external and internal policies on cyberspace. At the international level, India is usually cited as an example of how ICT can be deployed both for the well-being of the citizens as well as for promoting economic growth. This gives India also a substantial voice in global discussions on the use of ICT in development as well as a leadership position in the developing world on debates over related issues such as ICT governance. However, even as India is expected to articulate the developing countries position on cyberspace issues, the low level of awareness and priority given to it within the country has come in the way of developing positions on issues of contention.

International positions on cyberspace have largely been formulated by the line departments in the Ministry of Communication and Information Technology.[97] Representation in the international arena has largely been from the ranks of the Department of Electronics and Information Technology (DEITY), the National Security Council Secretariat (NSCS), and the Ministry of External Affairs.[98] This has also contributed to fragmented approach to cybersecurity dictated by different requirements and priorities at different points in time.

Most countries have published cybersecurity strategies that unite all the various aspects of cybersecurity into a coherent broad structural

---

[97] The ministry is itself a relatively recent addition to the ranks, having been established as the Ministry of Information Technology in 1999 and merged with the Ministry of Communications in 2001.

[98] As a case in point, India was represented in the 2004 UN GGE by a senior official from the NSCS, and in the 2010 GGE by a senior scientist from DEITY. The 2011 GGE has representation from the Ministry of External Affairs.

framework. These countries have also been able to revise, build and flesh out their strategies, based on both their experiences and in keeping with the rapidly changing technologies and the threats in the cyber domain. The Indian Government also embarked on this endeavour, and a draft policy was brought out by the Department of Information Technology in March 2011.[99] While measures to secure critical infrastructure and governmental networks found place in the policy, the absence of timelines and roadmaps made the policy more a manual of cybersecurity than a policy. The final version of the National Cyber Security Policy (NCSP) was released in June 2013, but it too has been criticised for many of the same deficiencies.

A comprehensive ICT policy that goes beyond the techno-centrism of the Ministry of Communication and Information Technology is lacking at the government level. The term more commonly used is 'e-governance' indicating the narrow focus on improving governance through the use of ICT. The central government's e-governance strategy is encapsulated in the National e-governance Plan of 2010.[100]. Prior to this, there had been many isolated endeavours at the state and central government level, and even private sector initiatives such as the *e-choupal*.[101] A similar scheme undertaken by the Karnataka state government was the *Bhoomi* initiative.[102] Both these initiatives suffered from similar drawbacks: lack of reliable connectivity, scarcity of end-use devices and lack of basic infrastructure such as electricity in the rural areas. Lack of standardisation and difficulties in scaling up were the other issues faced by, what were essentially, pilot projects. Similar travails may be expected with regard to cybersecurity that is necessary for effective e-governance in terms of ensuring security of data and individual privacy up and down the electronic pipeline.

---

[99] *Draft of the National Cyber Security Policy*, Department of Information Technology, March 26, 2011, p. 3.

[100] *National E-Governance Plan*, Government of India, at http://www.india.gov.in/govt/national_egov_plan.php (Accessed July 1, 2012).

[101] David M. Upton and Virginia A. Fuller, *ITC eChoupal Initiative,* Harvard Business School, January 2004, at http://cb.hbsp.harvard.edu/cb/product/604016-PDF-ENG (Accessed July 26, 2012)

[102] Keya Acharya, "Flaws in Bhoomi, India's model e-governance project"*, Infochange India,* July 2003, at http://infochangeindia.org/technology/features/flaws-in-bhoomi-indias-model-e-governance-project.html (Accessed July 27, 2012).

Another aspect of the ICT perspective is that the emphasis on information and communication technologies is not limited to cyberspace but also includes mobile phones, networks, space based Global Positioning Systems (GPSs ), etc.

## The Law Enforcement Perspective

The major debates on this perspective have revolved around whether this new domain of human activity can be regulated by existing laws, or new laws need to be enacted in view of its many unique characteristics. While the process around the creation of the IT Act 2000 also included the amendment of various existing laws, including the Indian Penal Code, it did not include provisions on cybercrime *per se*. It was only after the Mumbai attacks of 2008 that the government accelerated the process of amending the bill and then enacting it in 2009. The emphasis this time around was on cyberterrorism and cybercrime, and a number of amendments were made to existing sections and new sections added to take these threats into account.[103] In keeping with its focus on law enforcement and national security, the Act enhanced the powers of the government to intercept, monitor and block data through orders served on carriers and data hosting providers. This continued with several other rules being promulgated under the Act. These included the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 that require cyber café owners to keep records of identity and maintain logs of websites accessed by customers.[104] The Information Technology (intermediaries guidelines) Rules, 2011 focussed on national security and gave the Indian Government the right to force intermediaries, such as website hosting providers, to remove content and block websites without giving any reason, and without legal recourse. As in the case of the Cyber Cafe Law, the provisions are so vague that they can be interpreted any which

---

[103] In a panel discussion on cybersecurity at the Munich Security Conference in February 2011, the Indian National Security Advisor noted that the IT Act empowers the government to "scan Indian cyber space, detect incidents, audit practices, and protect critical and other infrastructure".

[104] Information Technology (Guidelines for Cyber Cafe) Rules, 2011. Ministry of Communications and Information Technology, at http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

way.[105] As far as the efficacy of such laws is concerned, to date nobody has been convicted under the cyber terror provisions.[106]

The two aspects that come to the fore are combating cybercrime and maintaining law and order. Both come with their own sets of issues. The fight against cybercrime depends largely on the awareness of the extent of the problem which in turn depends on authentic reporting. While other countries are reporting enormous losses because of cybercrime, such reports coming out of India are comparatively fewer. As a case in point, though the cybercrimes unit of the Bangalore Police receives over 200 complaints every year, statistics show that only 10 per cent have been solved and a majority of these are yet to be tried in the courts. The cases that did reach the courts are yet to be resolved since the perpetrators usually reside in third countries. Even in cases, where they are residents of the 30 odd countries, with which India has an MLAT, the lack of standardisation of cybercrime laws and resultant issues of dual criminality make prosecution difficult. Countries that are major sources of cybercrime, such as Nigeria, are also missing from the MLAT list.[107] The result is no different even in cases of cross-border cybercrimes in countries, with whom India has an MLAT. In the words of a law-enforcement professional:

---

[105] According to Rule 3, Sub Rule 2(b), "Users shall not host, display, upload, modify, publish, transmit, update or share any information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever." Sub Rule 2(c) forbids users from publishing anything that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation. The Information Technology (Intermediaries guidelines) Rules, 2011, at http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf (Accessed May 15, 2012).

[106] These provisions have also been described in media reports as akin to the censorship followed in China. "India Puts Tight Leash on Internet Free Speech", *New York Times*, April 27, 2011, at http://www.nytimes.com/2011/04/28/technology/28internet.html?_r=1&ref=asia (Accessed May 05, 2013).

[107] List of Countries with whom India Has MLATs, Central Bureau of Investigation, at http://cbi.nic.in/interpol/mlats.php Accessed on 12 June 2012

> In most of the cases, servers of the websites are located outside India. The standard procedure includes mutual legal assistance treaty (MLAT) in which we have to send the detail to the state police head who gets in touch with Ministry of Home Affairs (MHA). The MHA officials provide details of the cases to INTERPOL that later asks specific government agency to investigate. When the reply eventually comes, it is no less than two years. By that time any case would be dead for investigation.[108]

## *The Bangaluru exodus: a short case study*

A 26 year-old woman was robbed, raped and murdered in the Rakhine state of Myanmar. The riots that followed started around June 3, 2012 and left 80 dead and 80,000 displaced. Unrelated riots in Assam were sparked off on July 20, 2012. In the meantime, the rest of the Islamic world had begun to take notice of the events in Myanmar, and there were protests in many countries including Pakistan and Iran. A lot of the hate content, designed to inflame passion across the Islamic world began to pop up on the Internet at that time. The first attacks against Northeasterners took place on August 8, 2012 in Pune. The next incident took place on August 14, 2012 when a Tibetan youth was stabbed in Mysore, eventually leading to the Bangaluru exodus. The exodus itself was triggered more by text messages and less by social media.

The government's response to the disinformation or misinformation campaign was initiated on August 17, 2012 when the number of text messages was restricted to five a day. On the same day, the department of information technology issued an advisory to intermediaries that any inflammatory and hate comments against Northeasterners on websites should be removed. From the August 18 onwards, instructions were sent out on a daily basis to ISPs asking them to block various websites.

As far as the banned sites were concerned, they contained videos and pictures that had no connection with the captions and inflammatory

---

[108] "Cyber Police Dreads Crimes that Crosses National Boundaries", *Times of India*, July 23, 2012, at http://timesofindia.indiatimes.com/city/ahmedabad/Cyber-police-dreads-crimes-that-crosses-national-boundaries/articleshow/15103023.cms (Accessed August 15, 2012).

literature. One of the videos turned out to be an NDTV report uploaded by a Pakistani fundamentalist media group without any alterations other than the addition of an inflammatory caption at the beginning of the clip. Most of the blocked sites were related to the Myanmar incidents and not with Assam. According to Google's Transparency Report, Google received five requests from CERT-In, citing laws covering disruption of public order or ethnic offence laws, "to remove content from Google+, a Blogger blog, 64 YouTube videos, and 1759 comments associated with some YouTube videos". In response to the requests, they removed one video and restricted 47 YouTube Videos from local view, in addition to removing 12 YouTube comments and disabling local access to 3 Blogger blog posts.[109]

An analysis of a Wikipedia page—that was blocked—revealed that inflammatory content on the page had been added from IP addresses in West Asia. Even though this had been removed by Wikipedia's crowd sourced system of volunteer editors, it was still probably blocked on the basis that there were a large number of posts and tweets linked to it.

Investigators point out that text messages were used to communicate to reach people in their native languages which shows that the episode was a pre-meditated and well-coordinated conspiracy. But that in itself is not conclusive proof.

With regard to this particular episode, the law enforcement machinery found itself completely out of its depth because it deploys off-line mechanisms in the online world. While imposing a curfew might work off-line, its cyber equivalent of blocking URLs is completely ineffective since a thousand other copies of the content will spring up elsewhere.

## The National Security Perspective

Cybersecurity has been within the purview of the National Security Council since 2002 with the National Security Council Secretariat taking many cybersecurity initiatives and participating in international dialogues.

---

[109] Google Transparency Report, July- December 2012, at https://www.google.com/transparencyreport/removals/government/IN/?p=2012-12 (Accessed March 15, 2013).

The role of the National Security Council Secretariat as the locus of any discussions on cybersecurity and for bringing together the various stakeholders has been honed to perfection. But it has been less successful in the natural corollary of coordinating the actions required to translate talk into action. While the need for a cybersecurity coordinator at the National Security Council secretariat has been highlighted in successive reports, it is yet to be translated into action and may be seen as indicative of the absence of a national security approach, of the type evidenced in other countries. The emphasis continues to be on the law enforcement-based approach. While at the international level, a national security dominant perspective is seen as being excessively focussed on security to the detriment of the fundamental rights of the citizen, the increasing attacks in cyberspace cannot be countered simply by law enforcement. The increasing sophistication of cybercrimes and its linkages with cyberterrorism, the attacks on critical infrastructure and the persistent threats to governments and military networks require a coordinated and integrated response.

## Unfolding Threats

The low level of computer security, largely because of pirated software and the presence of patriotic hackers in the countries of the region, have made it an arena for low-level hacking and website defacement. The hidden hand of the intelligence agencies of these countries can be discerned in the so-called "cyber wars" that break out every now and then. This is also probably why such attacks have not crossed any red lines, despite threats to bring down the financial systems and attack critical infrastructure. Nearly all the upswings in defacements and hacking that normally follow a tit-for-tat pattern have ended in truces being called by the hackers on various sides. Though these defacements do not amount to anything more than digital graffiti, they prove that more grievous damage could be easily inflicted. More destructive attacks might also have taken place, but these have not been reported either because they are yet to be discovered or they have been discovered but not publicised. As observed in other parts of the world, the usual trajectory begins with hactivism and then advances to other activities ranging from espionage to attacks on critical infrastructure.

Evidence of advanced persistent threats embedded in sensitive Indian networks and systems has been presented through successive reports

both from India and abroad. While the evidence remains circumstantial and cannot be confirmed, in view of the scope for spoofing in cyberspace, the cumulative logic of means, motive, method and opportunity, all pointed to China even though there were suspicions that intelligence agencies of friendly countries were also carrying out similar activities. While the attackers have engaged in comparatively benign activities like espionage, their presence within the networks means that the networks are compromised and open to more destructive actions by the perpetrators.

The first known case of cyberespionage in India was targeted against Tibetan organisations based in India, as revealed in the Ghostnet Report of 2009.[110] Other instances of cyberespionage were brought to light by investigators in other countries, beginning with the Shadows in the Cloud Report [111] in 2010, followed by the Operation Shady Rat Report in 2011 released by an anti-virus company.[112] That trend continues to this day, with the recent revelations of the Red October Report in 2013.[113]

---

[110] "Tracking GhostNet: Investigating a Cyber Espionage Network", Sept. 1, 2009, at http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/ (Accessed June 02, 2010).

[111] "Shadows in the Cloud: Investigating Cyber Espionage 2.0 Joint Report", Information Warfare Monitor and Shadowserver Foundation, Toronto, 2010.

[112] Alpevorich,Dmitri, "Revealed: Operation Shady Rat: An investigation of Targeted Intrusions into 70+ Global Companies, Governments and Non-Profit Organizations during the Last 5 Years", McAfee, 2011, at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (Accessed January 15, 2012).

[113] "The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies", Kaspersky 2012, at http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (Accessed October 23, 2013).

*CHAPTER - IV*

# The Regional Scenario

Even though cybersecurity is a global issue, the regional linkages are equally important in more ways than one. Firstly, cybersecurity has ratcheted up the ladder of real threats in Asia more than other parts of the world. The number of attacks with politico-military objectives is on the rise, even as rules-of the-road in cyberspace are virtually non-existent, leading to a state of cyber insecurity. Cyber insecurity prevails for a number of reasons. In the first instance, many of the current hotspots in the world are located in Asia. There has been a concomitant increase in cyberattacks in the respective areas where these hotspots are located. Thus, a combination of existing fault lines and the easy access to cyberspace as a new means of perpetrating conflict is leading to increasing cyber insecurity in the region. Secondly, growth of cyberspace in Asia is unparalleled, leading to concomitant increase in the vulnerabilities. At the same time, compared to other parts of the world such as the Americas and Europe, the frameworks for collaboration are still in their infancy.

## A Snapshot of Asian Cyberspace

According to the latest statistics, 44 per cent of all Internet users, numbering nearly a billion people, are in Asia. At the same time, Internet penetration in Asia is 26.2 per cent as compared to the global average of 32.7 per cent.[114] Within Asia, China was first with an online population of 513 million, followed by India with 121 million and Japan with 101 million. The developed regions of North America, Europe and Oceania were nearly saturated with a penetration rate of 70 per cent. Online users are increasingly translating into offline clout, with a resultant say in everything from the development of standards and technologies to the success or failure of e-commerce undertakings.

---

[114] Internet World Stats, at http://www.internetworldstats.com/stats3.htm.

Other characteristics of Asian cyberspace include the following:

- The top five countries in terms of average broadband speeds are in Asia, led by Hong Kong. According to the latest "Akamai State of the Internet Report", Hong Kong was at the top spot with an average peak connection speed of 49.2 Mbps; South Korea was in the second place with 47.8 Mbps and Japan was in third place with 39.5 Mbps.[115]
- China is the hardware factory of the world with economies of scale and government policies ensuring that "Made-in-China" products beat their competitors. This has strategic implications especially in the cyber arena because of fears that such products, especially in sensitive areas such as networking might be compromised.
- India is the leader in IT services and software development, while other countries like the Philippines and Malaysia are also seeking to increase their global share in these sectors.
- According to a McKinsey report, cyberspace contributed 3.5 per cent to the economies of the 13 countries surveyed in 2011, including India and China.[116]. As Internet penetration increases, this would be expected to go up proportionately.
- Many countries in Asia also rely on the Internet for e-governance, with the Government of India alone, expected to spend about $ 33 billion on its flagship Unique Identity Programme by the time it is completed.
- Asia is also home to some of the larger 'cyber powers', which is currently a generic term that refers to actual or potential cyber capabilities on the basis of various indices. These include population and state of technological development.

---

[115] "Akamai State of the Internet Report", Akamai, August 1, 2012, at http://www.akamai.com/stateoftheinternet/ (Accessed September 21, 2012).

[116] James Manyika et al. (eds.), *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity,* Rep. McKinsey Global Institute, May 2011, at http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters (Accessed Sept. 15, 2012).

The attraction of cyberspace as a means of launching bloodless attacks has prompted powers both with and outside the region to use it to achieve politico-military objectives, which has unleashed a continuing cycle of retaliation and counter-retaliation.

In the face of this developing reality, the countries of the Asian region have been at the forefront of reshaping cyberspace in keeping with their perceptions and, in some cases, strategic priorities. While a country like North Korea has completely cut itself off from cyberspace, Iran is also on the way to developing a separate countrywide intranet that is separate from the Internet. While Saudi Arabia has only one gateway into the country where all data is filtered, China has a great firewall that also performs a similar function. Such restrictions serve the dual purpose of being virtual borders while also allowing for content monitoring under the guise of national security.

While Indian policymakers are aware of the issues and have responded with policies, legislation, organisations and mechanisms that have been put in place over a period of time, security analysts believe that this is still inadequate for meeting the challenges. This is because India is in a rough cyber neighbourhood. It has to balance its commitment to an open, secure and global cyberspace with the threats, in and through cyberspace, to its national security.

## *A snapshot of Cyber Conflict in Asia*

Cyberspace has become a natural adjunct of the many ongoing conflicts in Asia. The severity and escalation of cyber conflicts in this region is directly proportional to the hostilities offline. Current cyber flashpoints can be located throughout the length and breadth of Asia. It is apparent that the attacks are being carried out through the available infrastructure without respect to geographic boundaries. The involvement of technologically advanced powers, from both within and without the region, in the hostilities in West Asia have put this region at the frontline of cyber conflict, apart from being an indicator of emerging trends in cyber conflict.

In 2010, the Stuxnet malware was identified as the first "cyber-weapon" and its success in disabling Iranian centrifuges brought the issue of cybersecurity centre stage. Stuxnet was directed against the Iranian nuclear

programme, and suspicions of US and Israeli involvement were confirmed by subsequent reports. These suspicions arose in the first place because of the sophistication of the malware, which, experts declared, could only be engineered through the resources available to a nation state. It was the first large-scale attack on critical infrastructure that ran on Supervisory Control and Data Acquisition (SCADA) systems.[117] While there have always been concerns about supply chain integrity, Stuxnet showed how even existing vulnerabilities can be effectively utilised in cyber attacks. The national origin of companies assumes even more significance in this regard.

Off shoots of Stuxnet have surfaced with regularity since then; the Duqu worm was discovered in September 2011, followed in quick succession by the Mahdi, Gauss and Flame malware. While Flame, Duqu and Gauss were said to share their digital DNA with Stuxnet, being spread predominantly via USB sticks, their primary purpose seemed to be espionage, with their targets ranging from banking to governmental and energy networks. Flame, in particular, was notable for its modular character and its size, averaging 20 MB. Its capabilities ranged from recording Skype conversations and downloading information from smartphones to more mundane activities such as recording audio, screenshots, keystroke and network traffic recording. The Mahdi Trojan seemed to have different godfathers and was spread via phishing e-mails even though its purpose was also apparently espionage. Infections were reported from Iran, Israel, Afghanistan, the United Arab Emirates, Saudi Arabia, Syria, Lebanon and Egypt.[118]

In April 2012, there were reports of a new virus, Wiper, which was much more malicious, and wiped off the data from all computers that it infected. This virus largely affected networks in Iran. Four months later, the Shamoon virus was reported to have wiped off the data from 30,000 computers of the Saudi Arabian state oil company,

---

[117] According to one estimate, it took the equivalent of six man years and around 1.5 million dollars to develop.

[118] "Cyberwar on Iran more widespread than first thought, say researchers", *Guardian*, September 21, 2012, at http://www.guardian.co.uk/technology/2012/sep/21/cyberwar-iran-more-sophisticated (Accessed February 15, 2013).

Aramco, followed a week later by a similar attack on the networks of Ras Gas in Qatar, the second largest LNG company in the world.

In what has become the norm for such cyber attacks, despite the intensive investigations by anti-virus companies, the origins of the malware have remained largely in the realm of speculation and inference. While ownership of the Stuxnet (and by inference, its cousins Duqu, Flame and Gauss) malware was claimed by the Obama Administration for electoral purposes, the Shamoon virus is believed to be a reverse-engineered version of the Wiper virus unleashed by hackers loyal to the Iranian regime.[119] Each successive attack represents a relentless and rapid escalation in capabilities and intent on the part of the perpetrators.

Iran has shown how rapidly cyber capabilities can be acquired; from having virtually no capabilities before 2009, it has now gained significant expertise, and is using it. This is what the US is finding out to its cost, as US banks are subject to a sustained volley of Distributed Denial of Service (DDOS) attacks by a hacker group that calls itself the Izz ad-Din al-Qassam Cyber Fighters, but is believed to be Iran retaliating for cyber attacks on its infrastructure.[120] While the US has begun to raise cybersecurity-related issues with China in its strategic dialogues, there is no such scope in the case of Iran, which like the US, takes advantage of the 'plausible deniability' accorded by cyberspace. In other words, this is the online version of a low-intensity conflict, continuing endlessly till one or the other side ratchets up retaliation. The end result might well be different, if such a scenario is played out elsewhere since the absence of collateral damage in this case is largely afforded by the technical capabilities of the US.

---

[119] However, as David Betz notes, anonymity is as much a problem for the aggressor as it is for the target. Clues have been left in malware software both to misguide and to claim ownership.

D. Betz, *Cyberpower and International Security*, June 2012, at http://www.fpri.org/enotes/2012/201206.betz.cyberpower-international-security.pdf (Accessed December 13, 2012).

[120] "Bank Hacking Was the Work of Iranians, Officials Say", *New York Times*, January 8, 2013, at http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (Accessed December 15, 2013).

Hostilities between countries in East Asia are also mirrored in cyberspace, and China is a common factor in many of these conflicts. In the past year, there have been DDOS attacks—emanating from China—on the Philippines, Vietnam and Japan, and vice-versa. The dispute over the Scarborough Shoal/Huangyan Island saw cyber attacks between China and the Philippines in April/May 2012 followed by a similar showdown between Chinese and Vietnamese hackers in May, and attacks by Chinese hackers on Japanese websites following the territorial dispute over the Diaoyu/Senkaku Islands in September.[121]

Among the various protagonists in East Asia, North Korea has carried out an aggressive campaign against South Korea using every weapon in its arsenal and inflicting some real damage in the process.[122] South Korea presents an easy target, being one of the most wired countries in the world, while North Korea does not even present itself as a target, having no networks worth speaking of. While not much information is available about the size of North Korea's cyber corps, South Korean estimates are that it has doubled in the last few years and now numbers around 3,000.[123]

In terms of capabilities, China ranks ahead of the other powers in terms of both capabilities and potential. The People's Liberation Army (PLA) has integrated cyber warfare units since 2003 and has built up a huge cyber military edifice. According to reports, the third and fourth departments of the PLA, responsible for military intelligence, are among the most powerful bureaucracies, not just in the military, but in China,

---

[121] "Japanese Websites Come under Attack as Senkaku Squabble Continues", *Japan Times,* September 20, 2012, at http://www.japantimes.co.jp/text/nn20120920b7.html (Accessed September 25, 2012).

[122] The most severe of the cyberattacks took place in March 2013 when several banks and media houses were infected with a virus that deleted data from their systems. The malware was reported to be similar to Shamoon malware, earlier used against Saudi Aramco.

"South Korea Cyberattacks Hold Lessons", *Computerworld UK*, Mar. 20, at http://www.computerworlduk.com/news/security/3436305/south-korea-cyberattacks-hold-lessons-for-us/ (Accessed May 8, 2014).

[123] "N. Korea Commands 3,000-Strong Cyber Warfare Unit: Defector", *Yonhap*, June 1, 2011, at http://english.yonhapnews.co.kr/northkorea/2011/06/01/46/0401000000AEN20110601004200315F.HTML (Accessed March 23, 2012).

because of their access to every bit of information that criss-crosses China.[124]

Other countries of the region lag far behind the Chinese in incorporating cyber warfare into their general war fighting doctrines and building up capabilities. South Korea's national cybersecurity strategy declared cyberspace to be an operational domain that needed a state-level defence system. The National Intelligence Centre was tasked with coordinating cybersecurity along with the Korea Communications Commission (KCC). The KCC has focused on a defensive role that includes detecting, preventing and "responding to cyber assaults".[125] As with other US allies in the region, South Korea also places a lot of emphasis on extending the alliance to cover cyberspace.

In the case of Japan, in its Annual White Paper released in 2012, the Ministry of Defence listed "responding to cyber attacks" as one of its priority areas. The Japanese Self-Defence Forces (SDF) were tasked with defending not only their own networks but also with "accumulating advanced expertise and skills needed to tackle cyber attacks" so as to contribute to the government-wide response to cyber attacks.[126] In addition to cyber vandalism, intellectual property from Japanese companies has also been the target of hackers with a notable incident being the August 2011 hacking of Mitsubushi Heavy Industries as well as other technology firms.[127] In the same month, 480 members of the Japanese Diet had their e-mail accounts compromised and machines hijacked, with the hijacked machines, apparently, communicating with

---

124 M. Stokes and Jenny Lin, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, 2011, at http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

125 "S. Korea Charts Out National Cyber Security Strategy", Yonhap, August 8, 2011, at http://english.yonhapnews.co.kr/techscience/2011/08/08/45/0601000000AEN20110808006500320F.HTML (Accessed October 30, 2012).

126 Annual White Paper 2012, Ministry of Defence, Tokyo, Japan, at http://www.mod.go.jp/e/publ/w_paper/2012.html (Accessed September 26, 2012).

127 "Japan Defence Firm Mitsubishi Heavy in Cyber Attack", BBC, September 20, 2011, at http://www.bbc.co.uk/news/world-asia-pacific-14982906 (Accessed September 25, 2012).

a server in China.[128] In 2013, a sophisticated cyberespionage campaign that targeted entities in Japan was discovered by security researchers. Codenamed Deputy Dog, it was subsequently found to have targeted US Government entities, Defense Industrial Base (DIB) companies, law firms, Information Technology (IT) companies, mining companies, and Non-Governmental Organisations (NGOs).[129]

In September 2012, the Ministry of Defence announced that it would constitute a 100-strong cyber unit with a budget of ¥ 21.2 billion ($ 270 million) following the recommendations made by a panel constituted to study threats in cyberspace.[130]

The panel made a number of conceptual definitions, terming cyberspace a domain like air, sea, land and space. It was an essential infrastructure for the SDF to carry out their activities, and it was, therefore, their responsibility to secure it. They would have to partner with others, both domestically and internationally, and these partners could also be from the private sector.[131] Cyberattacks would be considered on a case-by-case basis, but if carried out as part of a military attack, Japan would respond in self-defence. While most US allies are seeking close cooperation with the US, it has entered into a cyber defence cooperation programme only with Australia, the only one outside of its programme with NATO.[132] In October 2013, the two countries

---

128 "Upper House Computers Also Hacked", *Asahi Shimbun*, November 3, 2011, at http://ajw.asahi.com/article/behind_news/social_affairs/AJ2011110316472 (Accessed September 25, 2012).

129 "Operation SnowMan: DeputyDog Actor Compromises US Veterans of Foreign Wars Website", FireEye Blog, Feb. 13, 2014, at http://www.fireeye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html#more-4514 (Accessed March 30, 2014).

130 This is out of a defence budget of ¥4.7 trillion.

"Japanese Defence Panel: Cyber Attacks Can Be Basis for Military Self Defense", *Computerworld,* September 9, 2012, at http://news.idg.no/cw/ art.cfm?id=409AA657-DC59-0780-FF139675AC1AAE62 (Accessed September 26, 2012).

131 *Toward Stable and Effective Use of Cyberspace,* Ministry of Defence Panel on Cybersecurity, Tokyo, Japan, 2012, at http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf (Accessed September 26, 2012).

132 Lolita Baldor, "Cyber Cooperation Added to US-Australia Treaty", *Businessweek,* September 15, 2012, at http://www.businessweek.com/ap/financialnews/D9POVN5G0.htm (Accessed September 27, 2012).

announced that they were setting up a joint Cyber Defence Policy Working Group to foster "increased cyber defense [*sic*] cooperation with the improvement of individual cyber capabilities and interoperability between the [Japan] Self-Defense [*sic*] forces and U.S. forces, which will also contribute to whole-of-government cybersecurity efforts".[133]

## Opinions on Cyber Warfare

The debates on cyber warfare range from the definition of cyber warfare to questions of whether the current activities in cyberspace come under the ambit of cyber war. There are also questions about whether existing laws and convention on war can be adapted to the new environment of cyber warfare.

In the context of cyber war, the basic principles that have governed definitions and responses to traditional war, such as proportionality, distinction and territory cannot be easily adapted to cyber war. The alternate view that this new form of warfare calls for new paradigms, as seen, most prominently, in the Chinese espousal of "Unrestricted Warfare" and increasingly being viewed as the future of warfare, has been decried by some academicians as lazy intellectual thinking and a sure recipe for global chaos.

### *Chinese View on Cyber Warfare*

The Chinese began to focus on cyber warfare soon after the 1991 Gulf War and following the American concept of the Revolution in Military Warfare (RMA) and Network Centric Warfare. The 1999 treatise, *Unrestricted Warfare*, written by two colonels of the PLA, was the clearest indication yet of the Chinese view of cyber warfare. The authors began by saying:

> Does a single "hacker" attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle? ... Obviously, proceeding with the traditional definition of war in mind, there is no longer any way to answer

---

[133] "U.S.-Japan Set Road Map for Next 20 Years amid Asian Threats", Bloomberg, Oct. 03, 2013, at <http://www.bloomberg.com/news/2013-10-03/u-s-japan-to-expand-military-ties-for-first-time-in-16-years.html (Accessed January 8, 2014).

> the above questions. When we suddenly realise that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare.
>
> If this name becomes established, this kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten.[134]

The study then went on to analyse the use of information technology in war conditions. It was assumed that the above questions were rhetorical and were being considered in the context of a declared war scenario. The Chinese have followed through on their head start in cyber warfare by implementing several ideas, from joint operations to special forces.

According to Dean Cheng, the PLA thinking on future wars is marked by three nons: non-contact, non-linear and non-symmetric.[135] Non-contact would include computer network operations "that will effectively nullify an opponent's forces without having to directly confront or engage them".[136] Following that a non-linear and non-symmetric war would take place in many dimensions, both physical and virtual, and not necessarily within a set battlefield or theatre. In view of this, the armed forces would require inter-service cooperation and shared situational awareness through advanced communication facilities. For shared situational awareness, information would have to be integrated into all aspects: from logistics, personnel, management to decision-making. The challenge will be to successfully overcome the vulnerabilities inherent in the digitising of the warfare landscape. Informationised warfare is therefore a competition between rival arrays

---

134 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare, (*Beijing: PLA Literature and Arts Publishing House, February 1999).

135 Dean Cheng, "The Chinese People's Liberation Army and Special Operations", *Special Warfare*, 25 (3), July-September 2012, at http://www.soc.mil/swcs/SWmag/archive/SW2503/SW2503TheChinesePeoplesLiberationArmy.html (Accessed August 15, 2013).

136 Ibid.

of information systems, and the side, with the more resilient and secure systems will prevail. While the focus of Western military planners is on accelerated decision-making through the use of technologies and concepts such as the *Observe, Orient, Decide and Act* OODA loop[137], they are constrained in their efforts to secure their networks, because of the differing capabilities and capacities of the allies. Conversely, the Chinese emphasis is on degrading hostile capabilities to the extent possible while at the same time securing their networks.

For the PLA, non-symmetric war justifies the use of methods such as hacking and the expropriating of intellectual property: 1) As a tool for getting access to and parity with the advanced technologies of the West 2) As part of psychological warfare (by visibly penetrating networks in other countries and raising the spectre of cyber instability)

By all accounts, some aspects of the air-sea battle concept recently publicised by the US Military, work along similar lines.[138] While the US military has been first off the block in declaring cyberspace as a war fighting domain, it is still struggling to formulate doctrines for cyber warfare in the light of its unique characteristics. The classified US Presidential Directive 20 issued in October 2012, which was leaked by the *Guardian* newspaper in June 2013, while discussing cyber operations and command and control, makes no mention of cyber weapons.[139] The Directive, however, noted:

> The United States Government shall integrate DCEO (Defensive Cyber Effect Operations) and OCEO (Offensive Cyber Effect

---

[137] The OODA loop was developed by USAF Col. John Boyd to explain the decision making process in a network enabled warfighting environment.

[138] Sydney Freedburg Jr, "Glimpse inside Air-Sea Battle: Nukes, Cyber at Its Heart", *Breaking Defence*, July 9, 2013, at http://breakingdefense.com/2013/07/09/glimpse-inside-air-sea-battle-nukes-cyber-at-its-heart (Accessed September 10, 2013).

[139] Martin Libicki notes in the context of nuclear weapons that before a device or a technique could be considered weaponised, hurdles of command and control, predictable effects and collateral damage, conformity with recognised norms of conduct, deployability in time and space, integration into combined arms, safety of storage and use, integrated logistics support and training. Many of these hurdles are applicable to cyber weapons as well though there are very few practical solutions.

Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, The Rand Corporation, 2007, p. 109.

> Operations) as appropriate, with other diplomatic, informational, military, economic, financial, intelligence, counterintelligence, and law enforcement options, taking into account costs, risks, potential consequences, foreign policy and other policy considerations.[140]

## Legitimising Cyber Warfare

The debates on cyber warfare range from the definition of cyber warfare to questions of whether any of the offensive actions seen so far in cyberspace come under the ambit of cyber war. There are also questions about whether existing laws and conventions on war, particularly the Law of Armed Conflict (LOAC) and International Humanitarian Law can be adapted to the new environment of cyber warfare. Military planners are also faced with the same conundrum since the assets they would have to defend in cyberspace consist of networks and data servers that are geographically dispersed, and in the case of cloud computing, there is a chance that both own and enemy assets could be on the same server. Other situations include that of being attacked by enemy-controlled botnets from within the country.

In this context, the conclusions of a group of law experts, brought out in the Tallinn Manual, is instructive. While coming out with a set of rules governing cyber conflict, derived from existing laws, there was no consensus within the group on whether any of these rules were applicable to the conflicts that had already taken place. None of the cyber incidents till 2012 had "been characterised by the international community" as reaching the threshold of an armed attack, be it the attacks on Estonia and Georgia or Stuxnet.[141] However, according to the group, the laws of armed conflict would be applicable in the case of cyber attacks during the Russia-Georgia War of 2008 since they

---

[140] However, OCEO and DCEO does not include "cyber collection", defined as operations for the primary purpose of collecting intelligence.

"Obama Tells Intelligence Chiefs to Draw up Cyber Target List – Full Document Text", *The Guardian*, June 07, 2013, at <http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text (Accessed November 8, 2013).

[141] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, p. 57.

were in conjunction with an on-going kinetic conflict.[142] In the case of the attacks on Estonia and Stuxnet, the "armed criterion" was difficult to establish in the absence of any kinetic conflict.[143] While Rule 13 states that the state has a right to self-defence in case of a cyber attack, and the scale and effects of the cyber operation determine whether it rises to the level of an armed attack; Rule 7 states that "the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State".[144] With no conclusive attribution still available for the attacks above, other than inferences and educated guesses arrived at after examining source code, this only serves to highlight the difficulties with adapting existing laws.

Given the blurred lines between civilian and military participation in hostilities, the Manual also attempted to provide a distinction between direct and indirect participation since civilian have always enjoyed protection under the laws of armed conflict so long as they did not directly participate in the conflict. According to the Manual, direct participation included 1) conducting cyber attacks and 2) Any actions which made possible specific attacks (e.g., identifying vulnerabilities or designing malware specifically to take advantage of particular identified vulnerabilities). Indirect participation included 1) Designing malware without the specific intention that it be used in the conflict and 2) Maintaining computer equipment generally, even if such equipment is subsequently used in the hostilities.[145]

---

142 Ibid., p. 76.

143 Ibid., p. 83.

144 Ibid., p. 34.

145 Ibid, p. 118-122.

*CHAPTER - V*

# CHALLENGES AND RESPONSES

## Challenges and Responses

### *Fashioning a Holistic Policy*

The National Cyber Security Policy (NCSP) was released in July 2013, and since then it has been proceeding in fits and starts. Despite the long gestation process, the policy was pilloried for falling short of spelling out concrete policies as well as for certain glaring omissions, such as the absence of a specific role for the armed services for ensuring India's cybersecurity.[146] In its defence, the National Security Council, which has brought out the Policy, has stated that the NSCP is only one part of a three-part framework including a National Cyber Security Architecture and a National Cyber Security Strategy (NCSS). Even as the other two legs are awaited, the policy itself has been fleshed out through the promulgation of guidelines, beginning with the Guidelines for Protection of National Critical Information Infrastructure with guidelines for other sectors under production.

A NCSS would perforce fill in the many existing lacunae and gaps in thinking on cybersecurity within the country. Firstly, even if it does not resolve the tensions between the various interests and priorities of different groups, be it the private sector, law enforcement, national security agencies or even Information Security (InfoSec) professionals, it would try to balance all these requirements to arrive at a consensus that is palatable to all stakeholders. Secondly, it would also give a sense and direction on the overall vision which is lacking at present.

The utility of an effective cybersecurity strategy may be seen in the strategies brought out by other countries. The US formulated its "National Strategy to Secure Cyberspace" in 2003, followed by the

---

[146] Bhairav Acharya, "The National Cyber Security Policy: Not a Real Policy*", ORF Cyber Monitor,* 1 (1), August 2013, at http://orfonline.org/cms/sites/orfonline/html/cyber/cybsec1.html (Accessed September 23, 2013).

"Comprehensive National Cyber security Initiative" in 2009. In his 2009 speech on "Securing Our Nation's Cyber Infrastructure", President Obama recounted the myriad uses of cyberspace, from connecting critical infrastructure to its uses by the military, economic and financial systems and the world wide web, and declared cyber infrastructure a "strategic national asset".[147] He termed the threat to this cyber infrastructure as "one of the most serious economic and national security challenges we face as a nation". He went on to say that "we will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage". Shortly afterwards, in 2010, the US Cyber Command was set up.

The UK Cyber Security Strategy of 2009 also highlighted the indispensability of this new domain for the effective functioning of government, business, critical infrastructure, as well as for the day-to-day activities of its citizens. It also underlined the many advantages of being an early adopter of a cybersecurity strategy including the good reputation enjoyed by UK networks which would encourage international businesses to set up subsidiaries in the UK; thus UK businesses would have the competitive edge in the global digital marketplace. It would also ensure the protection of the intellectual property of businesses and universities which underpins a knowledge economy. The strategy noted that the most serious and sophisticated threats came from state-sponsored activities, and these threats necessitated the strengthening of both civilian and military capabilities. The UK Government's National Security Strategy as well as its Defence and Security Review of 2010 placed primary emphasis on cybersecurity. Among the actions taken that year were the establishment of a Defence Cyber Operations Group with a budget of GBP 650 million as well as a cybersecurity test ranch to simulate cyber attacks.[148] During the 2012 Cyber security Summit in Budapest the UK government also

---

147 "Remarks by the President on Securing Our Nation's Cyber Infrastructure", The White House, May 29, 2009, at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (Accessed August 14, 2011).

148 "Defence Minister opens UK cyber security test range", UK MOD Press release, October 26, 2010, at http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/DefenceMinisterOpensUkCyberSecurityTestRange.htm.

announced its plans to create a Centre for Global Cyber-Security Capacity Building with an investment of GBP 2 million.[149]

Australia created its cybersecurity strategy in 2009 which led to the establishment of CERT Australia. A Cyber Security Operations Centre (CSOC) was also set up the same year, following the recommendations made in the Australian Government's Defence White Paper of 2009. A review of Australia's cybersecurity strategy published by the Kokoda Foundation think tank in February 2011 recommended that: a) government should determine a declaratory policy on how it will respond to attacks and b) that a minister be appointed with oversight responsibility for cyber issues. There have been recommendations that the 2009 Strategy needs to be updated to keep pace with rapidly evolving technological threats.[150]

Major cyber powers that have not declared their cybersecurity strategies include Russia and China. In their case, it is likely that the statist nature of the governments, where national security tops the agenda, obviates the need for a strategy.

## *Implementing the Cybersecurity Policy*

Even the most comprehensive policies listed above suffer from shortcomings, but the bigger problem in India lies in implementation. The draft of the cybersecurity policy listed a number of major stakeholders including the National Information Board (NIB); National Crisis Management Committee (NCMC); National Security Council Secretariat (NSCS); Ministry of Home Affairs (MHA); Ministry of Defence; Department of Information Technology; Department of Telecommunications; National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In); National Information Infrastructure Protection Centre (NIIPC); National Disaster Management Authority (NDMA); Standardisation, Testing

---

[149] "UK Announces Extra Funding for Cyber Security Capacity Building", Cabinet Office, October 4, 2012, at http://www.cabinetoffice.gov.uk/news/uk-announces-extra-funding-cyber-security-capacity-building (Accessed October 23, 2012).

[150] Kokoda Foundation, *Optimising Australia's response to the cyber challenge"* February 14, 2011 at http://www.kokodafoundation.org/Resources/Documents/KP14Responseto Cyber.pdf

and Quality Certification (STQC) Directorate and Sectoral CERTs; interestingly, these are just the governmental stakeholders.[151] While some agencies, such as the NDMA of India play only a peripheral role, and many of the sectoral CERTS are yet to be set up, the real responsibility for oversight over cybersecurity is of the ministries of communication and technology, home affairs, defence and the office of the National Security Advisor. The National Security Advisor's office has been actively engaged in putting in place a streamlined structure with lines of communication between all the major stakeholders and apex bodies both at the policymaking and operational levels. Steady progress has been made towards addressing the issue, and a number of working groups and committees have been set up within the government and across sectors. The problem however lies in implementation, not just at the central level, but also at the state level. The only tangible result of the efforts made so far has been the formulation of a Crisis Management Plan for cybersecurity. This is a bare bones manual that contains instructions pertaining to business continuity, disaster recovery, incident response and digital forensics, but whose implementation would require officers at the level of Chief Information Security Officer (CISO) in each organisation, as well as for the regular auditing of governance, risk and compliance, which is very rarely the case. A comprehensive cybersecurity architecture as envisioned by the National Security Advisor in his speech at the National Institute for Advanced Studies in Bangaluru in January 2012 would have to factor in huge manpower requirements and find innovative means to draw in this manpower.[152]

## *Public Private Partnership in Cybersecurity*

Even though there have been sporadic instances of cooperation, the public private partnership in cybersecurity had begun as early as 2005 when Nandkumar Sarvade, an Indian Police Service (IPS) officer was

---

[151] The multiplicity of actors is not a problem confined to India. A US Government document noted that there are as many as 14 agencies that are directly connected with the management of cybersecurity, including the departments of Defence, Homeland Security, Justice, Transportation, Energy and the Intelligence Community.

[152] "Shortage of Right People for National Security Jobs: NSA", *Hindustan Times,* January 22, 2013, at http://www.hindustantimes.com/India-news/Bangalore/Shortage-of-right-people-for-national-security-jobs-NSA/Article1-997948.aspx.

deputed to National Association of Software and Service Companies (NASSCOM) as Director, Cyber Security and Compliance.[153] Since there was a certain conflict of interest in an advocacy body such as NASSCOM to deal with regulatory issues, the Data Security Council of India (DSCI) was set up as an independent non-profit body in 2008.[154]

Close cooperation between the government and the private sector is necessary because much of the infrastructure and networks are in private hands. As the IDSA Report on cybersecurity noted:

> National security has traditionally been the sole responsibility of governments. But as the world has moved into the information age, with increased dependence on information infrastructure for production and delivery of products and services, the new responsibility of securing the critical information infrastructure (CII) against the rising number of cyber attacks has come within the ambit of national security. This new responsibility is not, however, solely that of government; and the private sector has a major role to play since more and more CII is owned and operated by it.

The government has accepted that this argument is not without merit. Accordingly, both the government and the private sector have been attempting to build bridges, and find ways and means to cooperate on cybersecurity. As a first step, a joint working group was established in July 2012 with representatives from various ministries of the Government of India and the private sector. The group came out with a report three months later, which identified the priority areas and recommended the setting up of a number of pilot projects. The road map included the creation of an institutional framework for, public private partnership, capacity building, setting security standards and

---

[153] Nandkumar Savade, 'Broken Windows in Cyberspace', *Police Chief Magazine*, 74 (3), March 2007, at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1134&issue_id=32007.

[154] "Council for Data Security", *Times of India*, June 25, 2007, at http://articles.timesofindia.indiatimes.com/2007-06-25/chandigarh/27976424_1_data-security-council-software-and-service-companies-place.

audits, apart from taking steps to fix supply chain vulnerabilities. In terms of concrete proposals, it called for the setting up of a few more committees, and capability building through an Information Sharing & Analyses Centre, the establishment of an Institute of Cyber Security Professionals of India as well as four pilot projects. These would include the setting up of a testing lab and a multi-disciplinary centre of excellence, undertaking a test audit and studying vulnerabilities in a sample critical information infrastructure. Though this is a step forward from the NCSP, it also suffers from many of the same infirmities, including the lack of a comprehensive road map with timelines, and not addressing the crucial issue of the funding of many important initiatives.

While the government acknowledges that this kind of intense collaboration with the private sector is a new experience, the private sector itself has to overcome many obstacles. There is a multiplicity of competitive actors within the private sector, with various industry organisations determined to play the dominant role. With membership of these associations consisting of both foreign and Indian companies, a trust issue also comes to the fore.[155] The government also expects private institutions to take up the slack in training the workshop needed for cybersecurity, in much the same way as it did for information technology.

## *Supply Chain Integrity*

In this unfolding situation that is marred by distrust, supply chain integrity has become paramount with the needle of suspicion pointing towards the hardware and software that make up the brains and body of cyberspace. While much of the equipment used in global networks is supplied by China, the storage and data storage networks are largely the domain of first mover companies based in the US, but are also dispersed across other developed countries. Many countries rely on trade control mechanisms to dissuade network providers from being excessively dependent on Chinese manufacturers, but such measures

---

[155] Saikat Datta, "Executive of Telecom Giant that Aided NSA Spying Is on India's Cyber Security Panel", *Hindustan Times*, 8 Apr. 2014, at http://www.hindustantimes.com/india-news/executive-of-telecom-giant-that-aided-nsa-spying-is-on-india-s-cyber-security-panel/article1-1205483.aspx (Accessed May 11, 2014).

have fallen foul of trade treaties; further, the competitive prices offered by Chinese manufacturers are big draw. Australia was one of the first countries to get exercised about the excessive use of Chinese-made equipment in Australian telecom and digital networks. This came to a head in 2009 when the Chinese manufacturer Huawei with supposed close links to the People's Liberation Army (PLA) was banned from bidding for the $ 38 billion National Broadband Network.

## The Hardware Sector- a case study of China and India

China is a major trading partner of India, with the bilateral trade going up from $ 2 billion to $ 73 billion in the course of a decade. Much of includes import of infrastructure equipment for the power and transport sectors, and crucially telecom hardware. India bought over $ 5 billion worth of Personal Computers (PCs) and mobiles, and another $ 13 billion worth of ICT manufactures including sub-assemblies, switches and routers from China in 2011.[156]

China has further sweetened the deal for Indian companies by providing soft loans for their expansion. A case in point is the $ 1.93 billion loan given to Reliance Communications in 2011 by a consortium led by the Bank of China. Chinese companies are able to beat other companies, both Indian and foreign, by offering the lowest possible prices and providing quality products. Indian intelligence agencies have noted that similar tactics have been used in neighbouring countries as well.[157]

Chinese manufacturers have about 20 per cent share of the Indian telecom market, while Indian telecom manufacturers have only a three per cent share. In some sectors such as 3G networks, the Chinese share can go up to 60 per cent. The Indian Government asked a number of its agencies to analyse the risks involved, and they have highlighted various issues. One report said Chinese vendors were "supplanting

---

[156] OECD figures. Of the total imports from China valued at $55 billion, ICT manufactures and five billion smart phones accounted for $13 billion.

[157] Joji Thomas Philip, "Intelligence Agencies Fear China is Trying to Encircle India via Tech Deals with Neighbouring Nations", *Economic Times*, January 23, 2013, at http://articles.economictimes.indiatimes.com/2013-01-23/news/365054791huawei-and-zte-nepal-telecom-telecom-and-internet-communication.

and not supplementing" indigenous players in India's telecom equipment manufacturing sector. Another report highlighted the vendors' reluctance to share technical information and the system keys of their products with Indian operators. (A subsequent report noted that these keys have been supplied to Indian companies.)[158] There have been a few instances of contracts being cancelled, but only by state-run telecom companies. Even here, the state-owned companies, such as BSNL, have complained that they are being singled out and not given a level playing field.

The preponderance of Chinese companies like Huawei and ZTE, that are reported to have close links with the Chinese Military, has been of concern to the government. This is in line with the similar concerns voiced by other countries.[159] The government has tried to use prescriptive policy measures to get companies to go down the preferred path. The National Telecom Policy of 2012 has set a target for domestic telecom equipment to meet Indian telecom sector demands, to the extent of 60-80 per cent, by 2020. The Ministry of Communications and Information Technology has repeatedly urged telecom companies to be aware of the vulnerabilities of their equipment and told them they would be held responsible and subject to penalties if the vulnerabilities are not addressed. Ironically enough, Huawei was the only company that came forward, when the government invited companies to collaborate with the Indian Institute of Science in Bangalore to develop a testing lab to check telecom equipment for malware.[160] However Felix Mohan, Chief Information Security Officer (CISO) of Airtel in his presentation on hardware and software vulnerabilities, made during the release of the IDSA Task Force Report on cybersecurity, said that even auditing and certification are also not foolproof since

---

158 Anupam Dasgupta, "Dragon in Your Dongle", *The Week,* September 1, 2012.

159 "Huawei Spies for China, Claims Ex-CIA Chief", *Times of India*, July 19, 2013, at http://articles.timesofindia.indiatimes.com/2013-07-19/security/40678109_1_chinese-telecoms-global-cyber-security-officer-giant-huawei.

160 Bharti Jain, "Home ministry May Seek Review of IISc-Huawei Pact to Set Up Telecom Lab", *Economic Times*, June 28, 2011, at http://articles.economictimes.indiatimes.com/2011-06-28/news/29722347_1_telecom-gear-chinese-telecom-telecom-equipment. Other companies did not come forward because of issues of intellectual property rights.

> If one model passes certification, that means all the models are certified. Then there are the patch attacks; a software or hardware might be certified as secure, but they need regular patching and the patches might be trojanised and make the equipment insecure. The third vulnerability is in the supply-chain and distribution network; while a particular piece might be sent to the test lab and certified as secure, there is nothing to stop insecure and trojaned equipment being sent to the company. So, while a policy might seem feasible at a theoretical level, it might not work out at the operational level.[161]

In addition to the widely reported issues with hidden backdoors in products and kill switches, it is also a fact that network equipment providers get access to sensitive information in the course of providing after sales support.

The same is true of software and Internet connectivity, but with the US as the dominant provider of services. The vulnerabilities of software and networks puts countries like India, which already have large numbers of Internet users, and are on the cusp of greater growth, in a vulnerable position. US companies dominate cyberspace by virtue of their first mover advantage and the innovation ecosystem that fosters the growth of such companies in clusters like the Silicon Valley. Companies such as Google, Skype, Yahoo and Microsoft have a large user base in India. The advantages enjoyed by such companies as far as the ability to innovate and scale up is such that no Indian company can hope to compete with them. Therefore till recently, the top 10 Internet companies in India were all American. Further, much of the data traffic that traverses through cyberspace touches US networks at some point, or is carried over these networks.

The Snowden revelations show that US intelligence agencies used this dominance in addition to their own resources and technological expertise to engage in "cyber scrutiny".[162] While it may be argued that

---

[161] "India's Cyber Security Challenges", Task Force Report, IDSA, May 2011.

[162] China is also attempting to make inroads into this sector with companies such as Tencent rolling out products such as WeChat globally. However, Chinese companies are constrained both by their reputation as well as their relative lack of innovation and production values.

all countries engage in this sort of activity, the deliberate weakening of standards and protocols in order to access data and communications and the misuse of US companies for similar purposes is a new and more troubling development, given the unlimited vulnerabilities inherent in software as compared to hardware.

## *National and International Interactions*

India has been active in bilateral and multilateral forums pertaining to cyberspace. Bilateral cybersecurity dialogues have been initiated with various countries including Japan, South Korea, the UK, France and the US as well as the European Union.[163]

However, the dialogue with the US has been the most comprehensive till date. It began as early as 2002 with the establishment of the Indo-US Forum Cyber Security Forum.[164] The motivation on the US side was to safeguard the interests of US companies who were outsourcing to India. The preface to the fact sheet of the 2006 meeting of the Cyber Security Forum noted:

> The U.S. and Indian Governments are intensifying on-going cooperation to address national security issues arising from the increasing interdependency of our critical network information systems involved in outsourced business processing, knowledge management, software development and enhanced inter-government interaction.[165]

On the Indian side, the emphasis was on capacity building and research and development. The joint statement at the end of President Bush's visit to India also declared that the two sides:

> […] recognised the importance of capacity building in cyber security and greater cooperation to secure their growing electronic

---

163 Annual Report 2011-2-12, Ministry of External Affairs, p. 150.

164 "Indo-US Cyberterrorism Initiative Plenary Meeting of Indo-US Cyber Security Forum", Ministry of External Affairs, April 30, 2002, at http://www.mea.gov.in/press-releases.htm?dtl/13416/IndoUS+Cyberterrorism+Initiative+Plenary+Meeting+of+IndoUS+Cyber+Security+Forum.

165 "U.S.-India Cyber Security Forum: Enhanced Cooperation to Safeguard Shared Information Infrastructures", US State Department, March 3, 2006, at http://2001-2009.state.gov/p/sca/rls/fs/2006/62530.htm (Accessed July 19, 2008).

> interdependencies, including to protect electronic transactions and critical infrastructure from cyber crime, terrorism and other malicious threats.[166]

This dialogue ground to a halt in 2006 following an espionage incident and since then cooperation has been spotty. However, in specific cases, after the 26/11 attacks, the FBI did help in tracing the Voice over Internet Protocol (VoIP) calls to their sources of origin and tracking the convoluted payments made for these services. India and the US signed a Memorandum of Understanding (MoU) on cybersecurity in July 2011.[167] The MoU established best practices for the exchange of critical cybersecurity information and expertise between the two governments through the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, and the United States Computer Emergency Readiness Team (US-CERT). The International Observer Programme of the U.S. Cyber Storm III, national cyber incident response exercise, in 2010, for the first time, included representatives from CERT-India.[168] The Indo-US Strategic Dialogue held in June 2013 renewed focus on cybersecurity with the establishment of a Strategic Cyber Policy Dialogue of cyber experts, looking at "cyber policy issues such as norms of responsible state behaviour [*sic*] in cyberspace, internet freedom, internet governance, and cybercrime cooperation", in addition to "whole-of-government Cybersecurity Consultations chaired by their respective national security councils to coordinate positions on cross-cutting cyber-security issues that impact international and economic security".[169] While the macro

---

166 India-US Joint Statement, Press Release, Prime Minister's Office, March 2, 2006, at http://pmindia.nic.in/press-details.php?nodeid=401 (Accessed March 10, 2012).

167 "United States and India Sign Cybersecurity Agreement", US Department of Homeland Security, July 19, 2011, at http://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement (Accessed September 18, 2012).

168 "Fact Sheet on U.S-India Strengthening Cooperation On Cybersecurity", White House, November 8, 2010, at http://www.whitehouse.gov/sites/default/files/Fact_Sheet_on_U.S-India_Strengthening_Cooperation_On_Cybersecurity.docx (Accessed March 15, 2011).

169 "U.S.-India Joint Fact Sheet: International Security", U.S. Department of State, June 24, 2013, at http://www.state.gov/r/pa/prs/ps/2013/06/211020.htm (Accessed October 5, 2013).

issues important to US are being addressed through these dialogues, they do not seem to provide scope for addressing issues important to India such as evolving the necessary mechanisms for rapid information sharing in the law enforcement process.

India has also been active at the multilateral level, particularly on issues of relating to Internet governance. In terms of material support, India hosted the 2008 Internet Governance Forum in Hyderabad. India also volunteered to host the Secretariat of the Government Advisory Committee (GAC) of ICANN, which it did, for five years till 2011. India has worked together with other emerging countries in the India-Brazil-South Africa (IBSA) Dialogue Forum to suggest alternate options for Internet governance. In 2011, India also proposed the setting up of a Committee on Internet-Related Policies (CIRP) to be based at the UN. Though there was a lot of criticism of the proposal, which was described as a UN takeover of the Internet, more reasonable observers noted that it was a response to the current disarray in Internet governance, and should be seen in that light.[170]

The consistency in this stand has continued right through to the NET mundial meeting where the representative from the Indian Ministry of External Affairs reiterated and justified a singular role for governments in internet governance in the following words:

> We recognize [*sic*] the important role that various stakeholders play in the cyber domain, and welcome involvement of all legitimate stakeholders in the deliberative and decision making process. Internet is used for transactions of core economic, civil and defence assets at national level and in the process, countries are placing their core national security interests in this medium. Now with such expansive coverage of States' activities through the internet, the role of the governments in the Internet governance, of course in close collaboration and consultation with other stakeholders is an imperative.

---

[170] Milton Mueller, *A United Nations Committee For Internet-Related Policies? A Fair Assessment*, Internet Governance Project Blog, October 11, 2011, at http://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for-internet-related-policies-a-fair-assessment/.

A hardening of stance on this account might be inevitable on account of two recent developments: 1) The revelations of mass surveillance by the US NSA which it was able to undertake with ease on account of the dominance of US companies in Internet services. 2) US intransigence in reducing the activities undertaken by the NSA as per the recommendations of successive commissions set up in this regard.[171]

## Engaging in the multi-stakeholder process

In addition to the private sector, the government has made efforts to engage with the civil society in the true spirit of multi-stakeholderism, with the most prominent instance being the India Internet Governance Conference held in 2012. Even though modelled on the lines of the Internet Governance Forum, it has proved to be a one-shot affair, with even the official website being removed of content. While there are many civil society groups and NGOs working in this field, they are widely dispersed and viewed with suspicion by the government since many of them receive funding from private sector companies and multinationals that are vested in this sector. In some cases, civil society groups have been virtually taken over by participants from industry.

## Protecting Indian cyberspace

CERT-IN began operations in 2004 with a mandate to "create a safe and secure cyber environment through appropriate policies and legal frameworks". Specific tasks included creating appropriate cybersecurity standards/guidelines, auditing, networking and points of contact, conducing cybersecurity drills, devising deploying Crisis Management Plans and Cyber Alert systems and interfacing with Sectoral and Foreign CERTS. The Mumbai Attacks of 1998 which were considerably cyber-enabled from conception to implementation prompted the Government to amend the IT Act in that year itself.[172] The Information Technology Amendment Act, 2008 provided for a national nodal

---

[171] White House,Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12 December 2013 Washington D.C.

[172] Investigations revealed that the terrorists had used Google Earth used for training and VOIP to communicate with their handlers; Garmin GPS units and satellite phones were also found in their possession.

agency for critical information infrastructure protection which has been set up after it was decided to make National Technical Research Organisation (NTRO) the nodal agency for critical infrastructure.[173] Section 70 of the IT Act, 2000 defines critical information infrastructure as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety". The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under the NTRO in 2013, almost five years after being incorporated in the IT Amendment Act, 2008. The increasing instances of state sponsored malicious activities would have been a factor in the creation of this organisation and situating it within the NTRO.

The organisation's official mandate is to "Protect critical infrastructure against cyber terrorism, cyber warfare and other threats". In pursuit of this mandate, it has been given all powers necessary including interception powers. Oversight is provided by an Advisory Council of 17 representatives from different agencies. It had identified the following as critical sectors: civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, communication, information technology, law enforcement, intelligence agencies, space and government networks.

There are a number of potential obstacles to the effective working of the NCIIPC. Compared to CERT-In, it is much less public facing which can prove to be a problem in an environment where much of the infrastructure rests in private hands. This creates problems not only in coordinating cybersecurity efforts but also for gauging the extent of the problem since private companies are reluctant to acknowledge that they have been attacked and more often than not do not report such attacks.[174]

---

[173] "Five-Year Plan in the Works to Revamp Cyber Security", *Times of India*, December 18, 2012.

[174] News of most attacks and incidents of cyberespionage, whether it be on Reliance, ONGC or ITC have invariably been reported by third parties. The companies concerned have not confirmed such attacks, and in some cases have denied these attacks ever occurred.

International relationships and coordination are also crucial to cybersecurity and the NCIIPC would have to work on building these relationships as well. With a number of new organisations envisioned under the National Cybersecurity Framework/Architecture, points of contact which are a major part of Confidence Building Measures would need to be incorporated into the architecture. With increasing dependence on cyber networks and threats to critical networks and cyber enabled infrastructure on the rise, the need for points of contact to minimise the risk of misunderstandings and misperceptions cannot be underscored enough.

## Cyber Command

Though the Indian Armed Forces have been asked repeatedly by the top political leadership about the need to develop defences against cyberattacks, they only play a limited role in the absence of an official policy on offensive actions.[175] That notwithstanding, the armed forces have been mulling the structures necessary to carry out operations in the new domain and according to reports, the navy will lead these efforts.[176]

There is a profusion of agencies, ranging from the Corps of Signals to the Army Computer Emergency Response Team (A-CERT), the IT Departments of the various HQs and the the Integrated Defence Staff (IDS). The Defence Information Assurance and Research Agency (DIARA) has been designated as the "nodal agency mandated to deal with all cyber security related issues of Tri Services and Ministry of Defence" according to a statement made by the defence minister in Parliament in 2010.[177] There has been no official role for the military in

---

[175] Subimal Bhattcharjee, in Ashley J. Tellis and Sean Mirski (eds.), *Crux of Asia: China, India, and the Emerging Global Order*, Carnegie Endowment for International Peace, Jan. 10, 2013, at http://carnegieendowment.org/2013/01/10/crux-of-asia-china-india-and-emerging-global-order/f0gw (Accessed June 2, 2013).

[176] "Indian Armed Forces Mulling Three Joint Commands ", *The Times of India*, Sept. 24, 2012, at http://articles.timesofindia.indiatimes.com/2012-09-24/india/34061038_1_aerospace-command-cyber-command-strategic-forces-command (Accessed June 2, 2013).

[177] "Hacking of Security Information", Press Information Bureau, Government of India, July 27, 2010, at http://pib.nic.in/newsite/erelease.aspx?relid=63588.

cybersecurity, other than that of protecting its own networks that have been reportedly penetrated on and off.[178] This, despite the Minister of Defence referring to cyber threats as a major threat to the nation in virtually every speech made to the apex military gathering, the Combined Commanders Conference over the past three years.[179]

With the cyber arena now recognised as a new domain of war, setting up a force competent to achieve the dual objectives of defending the country from cyber attacks in war and securing the military's network operations in peace requires considerable thought. While the Armed Forces have an advantage in that legacy issues will be kept to a minimum since many of the networking initiatives are only now bearing fruition, the fact remains that the Army, Navy and Air Force all have their own separate networks where common networks are being created in the interests of efficiency and jointness.[180]

In addition to the offensive and defensive aspects, cyberspace also plays a support function. This would entail training at the lower end and re-training at the higher end to incorporate such aspects into overall defence planning and preparedness. While signals have always been seen as a support function, and personnel treated as such, the unfolding environment calls for altered career graphs to draw and retain suitable manpower in a highly competitive environment.

While the Pentagon made waves in 2010 by declaring cyberspace as a new domain of warfare, the main purpose was to stand up men and allocate a budget. Even if the lion's share of the 2015 budget allocation request has gone to Cyber Command, the Army, Navy and Air Force

---

[178] The Corps of Signals describes itself as "the lead agency and nodal centre for information and cyber security both within the Defence Services and at the National level" on the Indian Army's website. See http://indianarmy.nic.in/Default3.aspx?MenuId=Qd7lMkEdWdE (Accessed November 15, 2012).

[179] "Antony Asks Army to Build Cyber Security Capabilities", *The New Indian Express*, Apr. 22, 2014, at http://www.newindianexpress.com/nation/Antony-Asks-Army-to-Build-Cyber-Security-Capabilities/2014/04/22/article2182471.ece (Accessed May 13, 2014).

[180] George Seffers, "Lightening the Workload for Cyber Command", *SIGNAL Magazine*, Apr. 3, 2014, at <http://www.afcea.org/content/?q=node/12599 (Accessed April 13, 2014).

have also begun to create the structure of a future Cyber Force. In the case of the Army, a military occupational specialty, the "cyber network defender" has been created with appropriate promotional avenues to encourage enlistment of people with a technical background as well as to encourage migration from other military occupational specialities.[181]

[181] "Army Graduates Its First Class of Cyber Network Defenders", *Defense Systems*, Dec. 09, 2013, at http://defensesystems.com/articles/2013/12/09/army-cyber-network-defender-graduation.aspx (Accessed February 5, 2014).

# Conclusion

The preceding examination of cybersecurity issues throws up different priorities and perspectives at global, regional and domestic levels.

At the global level, shorn of its complexities, the major issues surrounding cyberspace are cybersecurity at the operational/technical level, internet governance at the socio-political and intergovernmental level, and adapting existing laws and conventions to cyber conflict. The responsibility for cybersecurity is shifting from technical bodies to states even though most states are ill prepared to shoulder that responsibility. Cybersecurity is the outcome of having the requisite knowledge, capabilities and capacities to ensure full awareness and mastery over the domain. In the absence of this, it is all too easy to be lulled into a sense of complacency based on the perception that there are no major disruptions in systems.

From a technical standpoint, the history of cyberspace is a continuing story based on advancement in a number of technologies leading to disruptive innovation. These progressions have been encapsulated in three eponymous laws, viz. Moore's Law, according to which the processing power of a microchip doubles every 18 months as a consequence of which computers become faster and the price of a given level of computing power halves every 18 months; Gilder's Law which states that the total bandwidth of communication systems triples every twelve months and Metcalfe's Law which propounds that the value of a network is proportional to the square of the number of nodes: as a network grows, the value of being connected to it grows exponentially, while the cost per user remains the same or even reduces. Till such a time that these laws reach their endpoint, and the pace of technological innovation slows down, policymakers will be behind the curve in responding to the challenges of cybersecurity.

Even going by the conventional wisdom that the lack of a formal, hierarchical governance structure is what enabled cyberspace to expand and scale up, the fact remains that this is a vacuum that needs to be filled. Cyberspace itself is a challenge, being one part virtual, and one part physical, having many of the characteristics of a global commons

or a global public good, but denied that space by virtue of its increasing strategic significance. The jostling for dominance over cyberspace, or preventing any one country or entity from dominating, creates a governance vacuum which in turn impacts on cybersecurity and makes the task of securing cyberspace all the more difficult. This manoeuvring for dominance takes place at many levels, from internet related technologies to standards and protocols.

This jostling is more pronounced in internet governance which has consequently been in a state of stasis ever since a roadmap of sorts was laid out at the WSIS in 2003. However, there was some movement in terms of the Netmundial summit which took place in November 2013,

There are no easy solutions to the challenges thrown up by the various forms of cyber conflict. In fact, the effect is more akin to smoke and mirrors, with policymakers in most countries responding to the more visible hostile acts and responding to them, and that too in a piece-meal fashion, the various cybersecurity policies notwithstanding.

India's unfolding objectives in the cyber domain could be said to be to secure cyberspace domestically, extend the benefits of cyberspace regionally, and ensuring that it is a part of the rule making process globally. Securing cyberspace is proving to be a big challenge largely because government fiats and cybersecurity policies not withstanding, it is the law enforcement and judicial systems that are found wanting. Illegal activities in cyberspace, whether it be in the form of cyberespionage, or cybercrime, are adequately covered by laws but the law enforcement agencies lack even the most basic forensic capabilities to investigate such activities. This is not unique to India but sets apart the developing countries from the developed countries. A second shortcoming is that of domestic hardware manufacturers which necessitates the purchase of foreign hardware with all its attendant vulnerabilities even for sensitive projects where the project contract is in the hands of Indian software companies. While India is an IT superpower, it is not a cyber power in that there are very few software products that would enhance cybersecurity being manufactured by Indian companies. Knowledge and capabilities in technologies such as software encryption are severely lacking with the best minds either

working abroad or in the software development labs of multinational companies within the country.

While it is the responsibility of the government to identify such lacunae and take corrective measures, the government itself has proved to be an impediment, with various ministries at loggerheads, fiercely guarding their turfs, even at the expense of national security. The same also goes for the private sector, to an extent, with various industry associations claiming be the true representatives of stakeholders and undermining the others. This only served to justify the existing distrust of private companies in government, particularly in their ability to deliver the goods. Private companies, also opted to take the easy route, preferring to go in for joint ventures rather than putting money into research and development. Unless these various issues are resolved, co-operation between the government and the private sector which is crucial for securing cyberspace would stay in a state of suspended animation.

This requires an integrated study of all the various issues and how they impact on each other, rather than isolated and disjointed prescriptions. It requires policymakers to take a broader strategic view of cybersecurity, and get a head start on problems instead of simply responding to them. It also requires them to address a patchwork of priorities since the threats are infinite and constantly evolving at rapid speed.

Governments find themselves struggling to deal with the issue of cybersecurity. Given the current state of play in cybersecurity, it is not surprising that any discussion sooner or later ends up as a confusing mix of viewpoints on fundamental rights, privacy, law enforcement, human rights, globalisation and national security, thus leading to a gridlock. With the passage of time, differing perspectives and approaches are getting more and more entrenched, thus making the job of arriving at a consensus on contentious issues even more difficult. The resultant disarray has emboldened a variety of malicious actors (state, non-state and criminal) to take advantage of the situation, both at the national and international levels.

This monograph attempts to provide an overview of the the global, regional and domestic dynamics that impact cybersecurity today.

**Dr Cherian Samuel** is Assiciate Fellow at IDSA. He has written on various cyber security issues, including critical infrastructure protection, cyber resilience, cybercrime, and internet governance. He has also presented papers on these topics at seminars and round tables around the world as well as different fora in India. He was co-ordinator of the IDSA Task Force on Cyber Security which published a report on "India's Cyber Security Challenges" in March 2012.

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

**Institute for Defence Studies and Analyses**
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
E-mail: contactus@idsa.in Website: http://www.idsa.in