The Geopolitics of Cyber Espionage

Munish Sharma*

There is an intricate relationship between the methods of cyber espionage and the evolution of information and communications technology, of which information security is a key aspect. This article is an attempt to establish forward and backward linkages of cyber espionage. It examines the geopolitics, methods, role of information security technology and, most importantly, how the future of cyber espionage is being shaped by emerging technologies such as supercomputing, quantum computing and 'big data', from an Indian perspective.

Introduction

The recent debate over the massive surveillance programme being run by the National Security Agency (NSA) of the United States (US) has gained critical momentum among the members of strategic and academic community the world over. It is fascinating to note that the concept of political espionage is centuries old, in fact, as old as the technique of statecraft. In the present context, surveillance and espionage play a key role in the foreign policy making, which, in turn, is shaping the international relations amidst changing national security imperatives. It is need of the hour to gather intelligence using surveillance and reconnaissance techniques spread across the land, sea, air, space and cyberspace domains. National, economic and security interests in the era of globalization and technological advances have brought about a paradigm

* The author is a doctoral candidate at the Department of Geopolitics and International Relations, Manipal University.

ISSN 0976-1004 print

Journal of Defence Studies, Vol. 9, No. 1, January–March 2015, pp. 83–101

shift in geopolitics, which is about human-geography interaction. The unprecedented growth of rising economies from the developing world, rapid industrialization, rising demand for energy, expanding markets, depleting natural resources—all these add to the growing confrontation with respect to the access and control of resources, such as hydrocarbons, gold, uranium and rare earth elements. As the competition percolates into the economic domain, espionage targeting the business plans and strategies of competitors is the emerging reality.

The last decade and a half has witnessed an exponential rise in the use of Informational Technology (IT) including web-based applications offering email, social networking, instant messaging, search engines, banking, e-commerce, and so on. Furthermore, mobile telephony has changed the landscape of communication with integration of data transmission over wireless networks. The world today is interconnected in the cyber realm, that too in real time. The attack on the World Trade Centre in in New York in September 2001 brought a paradigm shift in the security perception of nation-states. Post the attacks, major emphasis was laid upon pre-emptive measures by security agencies to monitor suspicious activities. The monitoring of cyberspace has been a key element of the counter-terrorism strategy in order to break into suspicious communication, track financial transactions, surveillance of suspects, among other things. At the same time, the changing geopolitical imperatives and steeping competition in technology and economy is compelling nation-states to exercise their power in the cyberspace. This is carried out by all the means to get access to intellectual property, secure communication channels, data pertaining to national security, research in strategic areas, and so on. With the shift in technology paradigm, traditional means of espionage have advanced towards cyber espionage, and various organizations, such as government agencies, private companies and research institutions, are all facing the consequences; India being an integral part of the information age, is evidently no exception to this phenomena. A lot of effort is being made to develop technologies which enable intelligence agencies to extract valuable information from the massive amounts of data being generated every day. The US' NSA is being criticized for massive surveillance programme, since the documents leaked by Edward Snowden unveiled the operational details. In this context, the changing *modus operandi* and motives of espionage need to be assessed with respect to changing technological contours from an Indian perspective.

Cyber Espionage: Economic Imperatives?

One of the early instance of corporate espionage dates back to 1848 when Scottish botanist Robert Fortune was hired by the East India Company to smuggle tea plants from China to India, as China had a monopoly on tea plant cultivation. Since the surge of globalization, there have been numerous instances of corporate espionage such as Proctor and Gamble Vs Unilever (2001), Microsoft Vs Oracle (2000), and Opal Vs Volkswagen (1997).[1] The primary aim of corporate or industrial espionage is to gain access to trade secrets, marketing plans, production processes, and blue prints for research on new technologies. The convolution of Information and Technology and Communication Technology has diffused physical distances, enabling modern day corporations to have operations and markets dispersed across different time zones. As organizational functions became networked, the vulnerabilities of computer systems and networks were exposed through cyber-based attacks targeted not just at business disruption but also to gather strategic information.

There have been numerous instances of cyber espionage where economic imperatives are clearly evident. A massive cyber espionage ring came into picture in 2004 in the US, when hackers gained access to many defence computer networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and National Aeronautics and Space Administration (NASA). This series of carefully coordinated attacks on the computer networks and defence systems, which lasted probably for three years, was designated by the US government as Titan Rain Attacks.[2] It is considered to be a large scale, nation-wide cyber espionage assault. Since then a number of nation-states have reported incidents of breach of their networks for the purpose of espionage, for either political or economic interests.

In 2008, some of the US and Europe based energy companies, including British Petroleum, Royal Dutch Shell, Exxon Mobil, and ConocoPhilips faced cyber attacks which led to the loss of information regarding oil and gas field bids.[3] In 2009, the US reported a hack into the servers of defence contractor Lockheed Martin, which were housing information related to the Joint Strike Fighter Aircraft F-35. Investigators suspected the Chinese to be behind the attacks. The same year the computer systems of companies maintaining the three North American electricity grids were intruded into.[4] The gathered information pertaining to bids or weapon system designs could be leveraged in the interests of the state while competing for oil fields or development of indigenous

technology. The electricity grids form the core of Critical Infrastructure, and any disruption could have debilitating effect on the functioning as well as security of the nation-state. The instances of intrusion into the electricity grids is a matter of serious concern.

In a 2011 study, McAfee attributed an intrusion attempt labelled 'Night Dragon' to a Chinese Internet Protocol (IP) address and indicated that the intruders stole data from the computer systems of petrochemical companies. There are numerous cases of insiders, primarily employees of private companies, found carrying or in possession of proprietary information alleged to be transferring to China.[5] More recently in 2013, there was a report by the cyber security company Madiant stating that the Chinese People's Liberation Army (PLA)[6] is responsible for an array of cyber-attacks through a specialized Shanghai-based unit known as Unit Number 61398.[7] The growing IT capabilities of China and the intention to use cyber espionage, has raised alarm bells among the US policymakers. The US firmly believes that China to date has compromised a range of US networks, including those of the Department of Defense, defence contractors, and private enterprises.

In the case of cyber espionage, there is no feasible demarcation between political and economic imperatives. A detailed report was prepared by the CERT-Georgia, based on the analysis of Cyber Espionage incidents against the Georgian Government in 2011. It reported the use of advanced malicious software found collecting sensitive, confidential information about Georgian and American security documents and then uploading it to some of Command and Control Servers, linking the attack to Russian official security agencies.[8] It is evident that cyber is going to be an essential tool for nation-states to achieve their national security, political and economic objectives in the future. Therefore, irrespective of geography, economic status, political conditions, a nation-state with technical capability is inclined to use cyber espionage capabilities to advance its national interest.

Malwares as Cyber Espionage Tool

In 2012, the Kaspersky Lab had unveiled Flame, a massive cyber espionage operation, which had been able to infiltrate computers in West Asia and in significant numbers in India as well. It was dubbed as a highly sophisticated, malicious program by Kaspersky Lab, which discovered and investigated the code after the International Telecommunications Union (ITU) asked the Lab to look into it. Many computers belonging to the

Iranian Oil Ministry and the Iranian National Oil Company had been hit with malware that was stealing and deleting information from the systems. Flame was discovered in 2012, but it was alleged to be operating in the wild as early as March 2010, though it remained undetected by antivirus and security software.[9] The functionality of Flame is most interesting. It turns on the internal microphone of an infected machine to secretly record conversations that occur either over Skype or in the computer's near vicinity; a Bluetooth module which scans for other Bluetooth-enabled devices in the vicinity to siphon names and phone numbers from their contacts folder; and a module that grabs and stores frequent screenshots of activity on the machine, such as instant-messaging and email communications, and sends them via a covert SSL (Secure Socket Layer) channel to the attackers' command-and-control servers.[10]

The use of antivirus software is a common security measure to detect or thwart cyber-based malware through an array of vectors such as worms, viruses, Trojan horse, portable media, etc. The US-based companies hold around 36 per cent of the global antivirus market. The list includes Microsoft, Symantec and McAfee.[11] It is fascinating to note that it was a Russian antivirus firm—Kaspersky Lab—which unveiled the functionality and real intent of Stuxnet malware after it was found infecting some systems in Belarus. It might be a coincidence, or an act of deliberation, that none of the US-based antivirus firms began the investigation of malware after instances of infection were reported.

In 2013, the Kaspersky Lab unveiled a massive cyber espionage network named Red October. In the same year, the Lab identified a malware—named NetFile-801 (NetTraveler)—to be a major threat which impacted 350 organizations such as embassies, oil and gas corporations, and military contractors across 40 countries, including Russia, India and China.

Based on the report published by Kaspersky Lab, it is fascinating to note that different malware codes leave behind certain trails about their origin. For instance, comments in the Flame Command and Control were written in English, artefacts in Red October indicated Russian speakers, and NetTraveler indicated Chinese natives. Post Stuxnet, it was the discovery of Flame, which generated numerous questions on the manner in which malware is being used as a weapon or surveillance tool in cyberspace. It is quite evident that the prime targets of malwares are embassies, oil and gas corporations, military contractors and defence research organizations, all of which hold great strategic importance. A potent payload mounted on

malware is quite capable of not just penetrating the networks but lying within the network undetected, making it a cost effective method or tool of espionage in the cyberspace. As the malwares grow in number and sophistication, cryptographic means to secure stored information and communication channels could be an effective solution.

Cryptography, Encryption and Information Security

The information pertaining to matters of national security, economic development, foreign policy, business, research and development, etc., is stored, processed and disseminated over computer systems and networks. In the era of network centricity, the availability, confidentiality and integrity of information is vital to the decision-making process as information is an asset. The need to conduct private communication over public network or medium led to the evolution of cryptography.

The research on encryption in computer systems began primarily in the US during the 1970s, involving academia, industry and the government. The use of computers has made cryptography highly complex and the discipline needs expertise in mathematics and computer sciences. There are a number of published algorithms that are considered secure, including, but not limited to, Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5), and RSA (Rivest, Shamir and Adelman). Cryptography finds its application in Digital Rights Management (DRM) also, which has emerged as a controlling technique for copyrighted material, a boon for knowledge-based economies.

Cryptography forms the foundation of secure communication and computer security as encryption is employed at every stage of the communication process to maintain data confidentiality, integrity and authenticity. The privacy of data, messages and conversation is mandatory for electronic commerce, email, secure remote access, digital signatures, and security controls, among others. With the penetration of the Internet in every walk of life, it has become quite easy to eavesdrop and monitor communication. As a result, the last decade has witnessed a tremendous growth in the use of encryption technologies varying from businesses that wish to keep trade secrets private to consumers who wish to prevent unauthorized access to their credit cards. Cryptographic techniques for security information have been under the scanner since 1970s and attracted criticism for the development of backdoors in the standards

and algorithms. These backdoors could be exploited to gain access to the networks of the targeted organization, such as research laboratories, defence contractors, embassies, government offices, and corporations, where the software or hardware has been deployed thus posing a serious threat to the information pertaining to national governments.

The Geopolitics of Information Security: The Role of NSA

The signals intelligence agency of the US—the NSA—focuses on foreign surveillance and it runs one of the most advanced cryptanalysis[12] infrastructures in the world. The agency has been closely involved in the development process of encryption standards, along with National Institute of Standards and Technology (NIST). The development of DES began in the 1970s to address the computer security requirements of the US government. The cipher known as LUCIFER,[13] developed by the International Business Machines (IBM), underwent modification after technical consultations with the NSA, and was adopted as a standard in 1977.[14] There have been some controversies associated with the whole process of standardization and technical changes made to its design at the behest of NSA. For instance, the key size of the actual algorithm was 128 bits, but reduced to 56 bits for the DES. Although the algorithm accepts the 64-bit key as input, the remaining 8 bits are used for parity checking, which has no effect on the security of DES.[15] Moreover, many cryptanalysts have questioned the mysterious S-boxes, which have been designed in close consultation with the NSA and assumed to be a 'backdoor'[16], with which NSA could decrypt data encrypted with DES without the key.

In 2001, NIST established AES to be the specification for electronic data encryption. AES is being used for cryptographic needs up to the level of Top Secret information with varying key lengths of 128, 192 and 256 bits to protect national security systems.

In order to secure data transmission, RSA is one the most used public key cryptosystem standards. Random numbers are critical to most of the modern day cryptographic applications, such as session keys, public key generation, digital signatures, etc. An insecure random number generator can compromise the security of entire cryptographic system. In 2007, Bruce Schneier, a world renowned cryptographer, had raised suspicion on the involvement of NSA in the development of NIST standard: Dual

Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG), which is used by RSA, as a probable 'backdoor'.[17]

The dynamics of geopolitics compel the security agencies to perform massive cryptanalysis to break encryption codes of the adversary as well as friendly nations. The NSA has been trying to either influence international encryption standards covertly, or develop the code-breaking techniques, so that they have access to any information they perceive to be important. Each year, the agency spends $250 million alone on collaborating with US companies and building backdoors.[18] As the penetration and influence of the Internet grows, NSA wants to eavesdrop on the internet traffic through its data analysis tools like TUMULT, TURMOIL and TURBULENCE facilitated by the web service providers and equipment manufacturers.[19] The bulk of the NSA's efforts go towards breaking through the most widely used encryption methods like Secure Sockets Layer (SSL), Virtual Private Networks (VPNs), and smartphone encryption services. Most of the encryption-thwarting techniques fall under the umbrella of a highly classified and well-funded programme codenamed 'Bullrun'.[20] Since the advent of computer-based encryption techniques, it has been noticed that NSA has always tried to institute the industry standard of encryption while it has tried to block a number of academic papers about encryption.

The US-based networking equipment manufacturer Cisco has a vast product line including Datacenter products, Routers, Local Area Network (LAN) products, Virtual server platform, Voice over Internet Protocol (VoIP) and VPN. The German magazine *Der Spiegel*,[21] based on the leaked documents from former NSA contractor Edward Snowden, disclosed that NSA had backdoor to firewalls of Cisco, known as 'JETPLOW'. On similar lines, the malware 'FEEDTROUGH' was implanted in the products of Juniper Networks, another US-based manufacturer of networking equipments. Even Huawei, the Chinese manufacturer found the malware 'HEADWATER' implanted on its routers. The US has strong dominance in the global computer and networking hardware as well as in the software market. Firms like IBM, HP, Dell, Oracle, Cisco, Juniper Networks, Microsoft and NetApp have their products deployed in most of the countries, including India. Given the fact that the NSA has been working in tandem with such private firms, irrespective of any mode of encryption implementation,[22] the NSA could have access to a vast amount of Internet traffic.

The Future of Cyber Espionage

Since Edward Snowden unveiled the mass surveillance of the NSA, PRISM has been at the epicentre of global debate and criticism. Although, the interests of NSA in surveillance are as old as its existence, a major shift took place after the 9/11 attacks. There was a surge in the quest for intelligence pertaining to terrorists, their networks, communications, financial transactions, and any kind of activity deemed suspicious within the US or abroad. As a response to the electronic surveillance efforts of the US government, PRISM evolved as a tool used by the NSA to collect private electronic data belonging to the users of major internet services.

The efforts of the US government began under President George W. Bush with the Patriot Act, and expanded to include the Foreign Intelligence Surveillance Act (FISA), enacted in 2006 and 2007.[23] There was a reason the NSA was interested in the data on the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. In the age of Internet, every activity leaves behind a footprint as it is transmitted and stored on the servers in the form of email, video, photos, stored data, files stored on Cloud, VoIP, file transfers, or social networking details. However, there is another angle to it, as the same data could be used for business strategy by identifying potential customers, spotting fraud or cybercrime in its early stages, or improving products and services. Along with web service provides, the NSA has been gathering phone call details from wireless carriers such as AT&T and Verizon. A technician at AT&T in San Francisco reported on the existence of a secret room in the facility reserved for the NSA, and allowing the agency to copy and store millions of domestic and international phone calls routed through that station.[24]

This leads to the next question: how does NSA analyse this data and take out the desired information? What should be done with the millions of call detail records and electronic data? The gathered data, which runs into terabytes, needs to be structured and analysed to make sense out of it in the form of information. Here comes the role of analytics and 'Big Data'. The agency has partnerships with companies working in the domains of big data, analytics, cloud and supercomputing. The partnership with Palantir Technologies, is just one of many that the NSA and other agencies have forged as they have rushed to unlock the secrets of 'Big Data'.[25] The NSA used one such technology, known as Accumulo, a big data storage and application platform with better security via extremely granular access control[26] and massive scalability.[27] The technology was later launched to commercialize by the NSA developers.[28] As a result, it is not just the

agency, but private corporations which are able to gain economic mileage out of the developments. For instance, Accumulo makes it possible for companies to sift through massive amounts of information with essentially the same degree of sophistication and security as the country's top spy agency.[29]

The technology giant IBM has been working on supercomputing technology, and the resultant IBM Watson is a prime example of the power of data-intensive artificial intelligence. The Watson Ecosystem can interact in natural language where users can pose questions and get answers back with links to the relevant content from Watson's database.[30] The computing and analysis made by this technology would make it feasible to gain information from the massive data gathered by the NSA, which has been testing Watson over the last two years.[31]

Advances in Quantum Computing[32] technology will lead to development of path-breaking applications in the science of data analysis. This technology will enable data superposition[33] and entanglement.[34] If developed, computers based on Quantum Mechanics are going to revolutionize data analysis and optimization for a cross section of applications, such as air traffic control, protein modelling, weather prediction, database querying, and hacking tough encryption schemes. The RSA encryption relies completely on the factoring problem. Multiplying two large numbers is easy for any computer. Calculating the factors of a very large (for example, 500-digit) numbers, however, is considered impossible for any classical computer. In order to make the quantum leap, the NSA is investing heavily in this technology that has a strategic application to break nearly every kind of encryption used to protect banking, medical, business and government records around the world. Based on the leaked documents, it is being carried out under the aegis of a $79.7 million research programme entitled 'Penetrating Hard Targets'. What drives this is the fact that the application of quantum technologies to encryption algorithms threatens to dramatically impact the US government's ability to both protect its communications and eavesdrop on the communications of foreign governments.[35]

Cyber Espionage and India

As the instances of malware infections grow in number and sophistication, it is evident from the investigations that nation-states are actively involved in cyber-based espionage to secure their economic interests under the auspices of national interest or security. In an interview, the former NSA

contractor Edward Snowden stated that the agency is also involved in industrial espionage. As per the documents provided by Snowden to the *The Hindu*, the agency had also carried out intelligence gathering activities in India. The agency was using its 'Boundless Informant' programme to monitor telephone calls and access to the Internet in India. The controversial surveillance program 'PRISM' collected information through Google, Microsoft, Facebook, Yahoo, Apple, YouTube, and several other web-based services. This establishes the camaraderie between the NSA and US based technology firms.

India has been importing its telecom network equipment, and in recent times the Chinese equipment maker Huawei has outplayed big players. In 2014, an incident of hacking was reported wherein Huawei has been alleged to bring down the Base Station Controller of the Bharat Sanchar Nigam Ltd (BSNL) network in Andhra Pradesh. It is noteworthy that BSNL had given the contract to ZTE, another Chinese telecom equipment manufacture, for expansion in the state. There are two angles to this incident, one that inter-corporate rivalry of foreign firms has moved on to Indian soil and the other that such intrusion into the telecom network poses grave security concerns, given the fact that India is a major market for Chinese telecom equipment manufacturers.

An analysis of the recent malware infections clearly denotes that owing to the lack of security awareness India has been a soft target. The Stuxnet malware was found to have infected around 10,000 computers in India and some of them were located in facilities which were part of the critical infrastructure. The NetTraveler spear-phishing attacks exploited known vulnerabilities in Microsoft Office, targeting Indian users with emails carrying files entitled: 'Army Cyber Security Policy 2013.doc', 'Jallianwala Bagh Massacre a Deeply Shameful Act.doc', 'BJP Won't Dump Modi for Nitish: NDA Headed for Split.doc', and so on.

India has not merely been a victim of cyber-based espionage tools. The senior management of Norwegian telecom giant Telenor (the company was operating in India under the brand Uninor, in a joint venture with Unitech) reported spear-phishing incidents and the further investigation into the malware samples unfolded operation 'HangOver'. This was targeted at the business, government and political organizations, including targets of national security interest from Pakistan, separatist groups from India, and companies from different industries. There had been no reported incidents of such activity originating from India but based upon the analysis Norway's IT Security Company Norman stated

that this operation appears to originate in India, and interestingly it combines national interest targets with economic targets.

According to media reports, the Government of India (GoI) is going to deploy the internet spy system 'Netra'[36] which will sneak into voice traffic passing through widely used applications like Skype or Google Talk, write-ups in tweets, status updates, emails, instant messaging transcripts, internet calls, blogs and fora. This deep search surveillance system being set up by C-DoT, will be capable of monitoring and delivering Intercept Related Information (IRI)[37] across 900 million mobile (GSM and CDMA[38]) and fixed (PSTN[39]) lines as well as 160 million Internet users, on a 'real time' basis through secure ethernet leased lines.

The digital revolution led by Information and Communication Technology (ICT) has not merely increased the speed and reach of information, it has brought to the fore many a challenge to national security as potent threats are looming in the cyber domain. The adversary is technically well-equipped, the nature of warfare is asymmetric, and in the networked world targets could be reached remotely for espionage or attack. There is a huge economic cost associated with the breaches. The targets of espionage vary from embassies to research and development institutions, labs of strategic importance to private sector firms in energy or high-technology sector. Along with a national security threat, it is a major threat to intellectual property of any knowledge-driven economy.

India has been on a high economic growth trajectory in the last two decades. The interaction with the world has been increasing and so is integration in terms of capital and goods flows, people-to-people contacts, exchange of ideas, and, most importantly, the penetration of technology. In the present context, the societal functions varying from dispersal of governmental services to transportation and healthcare to energy are highly dependent on technology. As a result, the need for enhanced security is emerging as a daunting task because the growth and trajectory of technology is highly unpredictable. The sudden rise in the degree of sophistication of threats has opened up many frontiers where traditional security intersects with the non-traditional security imperatives. As a nation-state, we are neither isolated from the merits of technology nor from the perils. The recent incidents of the use of cyberspace for espionage, as highlighted earlier, raise grave security concerns for India. The use of malware to exploit the vulnerabilities lying within the computer networks, applications, hardware, software, operating systems, protocols, etc., will intensify in the foreseeable future. If the US can develop such capabilities,

which may or may not be targeted at India, any nation-state having fair skill set in this domain is equally capable of developing and deploying malware to forward its interests.

India has a vibrant software development industry. As per NASSCOM[40] estimates, the Information Technology and Business Process Outsourcing industry exports would touch $84 billion by the end of the 2014–15 financial year. But the fact remains that India's IT sector is services-oriented, with volume of the work being software development and testing. The skill development in the IT sector has been based upon the outsourced IT requirements of the businesses rather than on innovation. The Indian IT sector has not been able to develop products and services which could compete with the technology giants like Google, MicroSoft, HP, Yahoo and Cisco. Very few Indian companies feature in the security products and networking equipment manufacturing market.

India imports majority of its telecom and networking hardware as well as software. These are either already operational or part of the expansion plans of telecom service providers operating in India. This presents a major concern because vulnerabilities in the systems could be exploited for intrusion, eavesdropping, disruptions or even attacks, which bear severe national security implications. It is evident from the above discussion that foreign intelligence agencies are using every means to exploit the vulnerabilities, either known in public or deliberately kept in a clandestine manner using backdoors. Moreover, Internet traffic is being monitored through web services while switches and routers give access to voice and data communication. On the other hand, the means to secure communication—encryption—has controversies lined up, whether in standardization process or weak keys or mysterious boxes alleged to be backdoors. The antivirus software used to detect and remove malware is under scrutiny to check whether it allows the state-sponsored malware to go undetected or not.

Conclusion

The rise of India and China as global economic powers has not just accelerated the competition between them for the control of resources, the possibility of their confrontation with the Western powers over strategic issues cannot be ruled out in the foreseeable future. In the case of China, we are already witnessing its confrontation with the US. The controversy over the alleged snooping by NSA clearly highlights that eavesdropping on foreign networks and Internet traffic is not a conspiracy theory anymore,

but a reality. The agency has been working closely with the web service providers that host majority of the email and messaging services, social networking platforms and electronic commerce. These service providers have a deep penetration in the Indian market comprising both private and business communication. Most of the corporate houses have deployed Microsoft Office tools for office automation and email communication. The data in email servers, although encrypted, could easily be made accessible to the NSA, opening up a window for corporate espionage. The alleged hacking by the Chinese telecom vendors into the communication networks of Indian telecom service providers increases the possibility of the use of such capability for espionage.

The growing capability of China in the cyber domain, both in numbers as well as quality, is going to be a major concern for India. China has been able to penetrate into the networks of defence contractors and oil companies of the US. It has been able to develop the skill set and resources to engage in a cyber espionage operation. The intention of China to use this capability against the adversary is clearly evident from the cases discussed earlier in the article as well as from recent developments. In February 2014, Chinese President Xi Jinping articulated the aspirations of China to be a 'cyber power'. The President is going to head the newly formed government body, a working group on cyber and information security.

The solution to all the above concerns points into one direction: indigenous development of hardware, software and standards. Cost-effective equipment, primarily from China, is penetrating the Indian market while domestic players are not able to meet either the quality or requirements of the technologically advanced users. The domestic demand of computer and networking hardware and software, at least in the critical infrastructure sectors, should be met by domestic production. Official communication should be highly restricted to government authorized service providers. The organizations that are part of critical infrastructure should be made to follow stringent security policies, controls, baselines in order to harden the targets.

In the meantime, stringent import policies on networking equipment with scrutiny and thorough testing of source code or hardware components could be a workaround. In the long run, there is a need for partnership with friendly nations having good technological and fundamental research infrastructure. Russia, with its expertise in mathematics and sciences, is an ideal partner for India to develop encryption algorithms, standards

and communication hardware. India needs a strategic partner in the cyber domain, despite the fact that there is no demarcation between friend and foe as friendly nations are also involved in espionage against each other. If India and Russia can collaborate in research over strategic matters like defence, there are vast opportunities for joint research and development in the field of information security too. After all, a secure cyberspace comprised of secure communication infrastructure is going to be critical to our national security in the future.

Notes

1. See 'Famous Cases of Corporate Espionage', *Businessweek.com*, available at http://images.businessweek.com/slideshows/20110919/famous-cases-of-corporate-espionage#slide1,accessed on 5 February 2014.
2. Thornburgh, Nathan, 'Inside the Chinese Hack Attack', *Time*, 25 August 2005, available at http://content.time.com/time/nation/article/0,8599,1098371,00.html, accessed 5 February 2014.
3. Clayton, Mark, 'US Oil Industry Hit by Cyberattacks: Was China Involved?', *Christian Science Monitor.com*, 25 January 2010, available at http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved, and Michael Riley, 'Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers', *Bloomberg*, 24 Februarey 2001, available at http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html, accessed on 6 February 2014.
4. 'Five Serious Cases of Cyberespionage', *Foxnews.com*, 22 April 2009, available at http://www.foxnews.com/story/2009/04/22/five-serious-cases-cyberespionage/, accessed 5 February 2014.
5. Wendell, Minnick, 'Chinese Cyber-espionage Growing', *DefenseNews.com*, 6 November 2011, available at http://www.defensenews.com/article/20111106/DEFSECT04/111060302/Chinese-Cyber-Espionage-Growing-U-S-Report, accessed 5 February 2014.
6. China's 2nd Bureau of the People's Liberation Army (PLA), General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).
7. 'US-China Cyber Espionage Comes Under Increased Scrutiny', *RT.com*, 7 November 2013, available at http://rt.com/op-edge/us-china-cyber-espionage-371/ and Dan McWhorter, 'MandiantExposes APT 1', *Mandiant.com*, 18 February 2013, available at https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/, accessed on 10 February 2014.
8. 'Cyber Espionage Against Georgian Government', Data Exchange Agency,

Ministry of Justice, Georgia, October 2012, available at http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf, accessed 10 February 2014.

9. 'Kaspersky Lab and ITU Research Reveals New Advanced Threat', *Kaspersky.com*, 28 May 2012, available at http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat, accessed 10 February 2014.
10. Zetter, Kim, 'Flame: The Massive Spy Malware Infiltrating Iranian Computers', *Gizmodo India*, 29 May 2012, available at http://www.gizmodo.in/news/Meet-Flame-The-Massive-Spy-Malware-Infiltrating-Iranian-Computers/articleshow/19159416.cms, accessed 10 February 2014.
11. 'Antivirus and Encryption: October 2013 Market Share Reports', available at http://www.opswat.com/about/media/reports/antivirus-october-2013, accessed 10 February 2014.
12. Cryptanalysis is the art of deciphering encrypted communications without knowing the proper keys. The objects of cryptanalysts are to read the text of encrypted messages and to recover the cryptographic systems used. There are many cryptanalytic techniques such as Ciphertext-only attack, Known-plaintext attack, Chosen-plaintext attack, among others.
13. In the late 1960s, IBM had set up a cryptography research group, headed by cryptographer Horst Feistel. The group created an encryption method named 'Lucifer' to protect the data for a cash-dispensing system that IBM had developed for Lloyds Bank in the United Kingdom.
14. See 'Cryptography for a Connected World', available at http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/, accessed 12 February 2014.
15. Kaufman, Charlie, Radia Perlman and Mike Speciner, *Network Security*, New Delhi: Pearson Education, 2005, p. 63. Also see Arthur Sorkin, 'Lucifer, A Cryptographic Algorithm', Lawrence Livermore Laboratory, April 1983, available at http://fuseki.com/lucifer.pdf, accessed 12 February 2014.
16. Gargiulo, Joe, 'S-Box Modifications and their Effects in DES-like Encryption Systems', SANS Institute InfoSec Reading Room, July 2002, available at https://www.sans.org/reading-room/whitepapers/vpns/s-box-modifications-effect-des-like-encryption-systems-768. Also see 'Data Encryption Standard', available at http://www-math.ucdenver.edu/~wcherowi/courses/m5410/des.pdf, accessed 12 February 2014.
17. Pauli, Darren, 'Leaked NSA Docs Suggest Dual_EC_DEBG Backdoor', *IT News*, 11 September 2013, available at http://www.itnews.com.au/News/356751,leaked-nsa-docs-suggest-dualecdrbg-backdoor.aspx, accessed 15 February 2014.
18. Ball, James, 'How US and UK Spy Agencies Defeat Internet Privacy and

Security', *The Guardian*, 6 September 2013, available at http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, and Adam Clark, 'The NSA Can Beat Almost Any Type of Encryption', *Gizmodo.com*, 5 September 2013, available at http://gizmodo.com/the-nsa-can-crack-almost-any-type-of-encryption-1258954266, accessed 15 February 2014.

19. Schneier, Bruce, 'How the NSA Targets Users' Online Anonymity', *The Guardian*, 4 October 2013, available at http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, accessed15 February 2014.
20. 'Secret Documents Reveal NSA Campaign Against Encryption', *The New York Times*, 5 September 2013, available at http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0. Also see, 'Project Bullrun—Classification Guide to the NSA's Decryption Program', available at http://edward-snowden.net/project-bullrun-classification-guide-to-the-nsas-decryption-program/, accessed 16 February 2014.
21. Appelbaum, Jacob, Judith Horchert and Christian Stöcker, 'Catalog Reveals NSA Has Back Doors for Numerous Devices', *Der Spiegel*, 29 December 2013, available at http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html and Kim Zetter, 'NSA Hackers Get the "Ungettable" with Rich Catalog of Custom Tools', *Wired.com*, 30 December 2013, available at http://www.wired.com/threatlevel/2013/12/nsa-hacking-catalogue/, accessed on 16 February 2014.
22. Encryption could be implemented either in hardware or software, while the latter option is generally less expensive and easy to install.
23. Sottek, T.C. and Joshua Kopstein, 'Everything You Need to Know About PRISM', *The Verge.com*, 17 July 2013, available at http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, accessed on 20 February 2014.
24. Risen, James 'How the US Uses Technology to Mine More Data More Quickly', *The New York Times*, 8 June 2013, available at http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&_r=0, accessed 20 February 2014.
25. Ibid.
26. Access control refers to security features that control who can access resources in the operating system. Applications call access control functions to set who can access specific resources or control access to resources provided by the application. The ability to enforce granular access controls gives the administrator the power to provide employees, partners, and clients with remote access to very specific and defined resources, according to the needs

of each user. It enables user's roles and responsibilities to be set so that individuals are given access only to relevant areas or functions of the system.

27. Scalable hardware or software can expand to support increasing workloads. This capability allows computer equipment and software programs to grow over time, rather than needing to be replaced. Scalable software refers to business applications that can adapt to support an increasing amount of data or a growing number of users.
28. Marko, Kurt, 'The NSA and Big Data', *Information Week*, 18 July 2013, http://www.informationweek.com/big-data/big-data-analytics/the-nsa-and-big-data-what-it-can-learn/d/d-id/1110818?, accessed 20 February 2014.
29. Smith, Gerry and Ben Hallman, 'NSA Spying Controversy Highlights Embrace of Big Data', *Huffington Post*, 6 December 2013, available at http://www.huffingtonpost.com/2013/06/12/nsa-big-data_n_3423482.html, accessed 22 February 2014.
30. 'Announcing the IBM Watson Ecosystem Program', available at http://www-03.ibm.com/innovation/us/watson/index.shtml, accessed 25 February 2014.
31. Bufithis, Gregory P. and Eric De Grasse, 'Surveillance, PRISM, Cybersecurity, IBM Watson, Privacy', available at http://www.projectcounsel.com/?p=2359, accessed 27 February 2014.
32. Quantum computing is essentially harnessing and exploiting the laws of quantum mechanics to process information. A traditional computer uses long strings of 'bits' which encode either a zero or a one. A quantum computer uses quantum bits, or qubits, a quantum system that encodes the zero and the one into two distinguishable quantum states.
33. Superposition is essentially the ability of a quantum system to be in multiple states at the same time.
34. Entanglement is an extremely strong correlation that exists between quantum particles, which could be so strong that two or more quantum particles can be inextricably linked in perfect unison even if separated by great distances. The particles remain perfectly correlated even if separated by great distances.
35. Rich, Steven 'NSA Seeks to Build Quantum Computer that Could Crack Most Types of Encryption', *Washington Post*, 2 January 2014, available at http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, accessed on 27 February 2014.
36. The 'Netra' Internet spy system has been developed by Centre for Artificial Intelligence and Robotics (CAIR), a lab under the Defence Research and Development Organization (DRDO).
37. Lawful Interception targets two types of data: (a) the actual contents of communications which may include voice, video or text message contents.

(b) Intercept Related Information: consists of information about the targeted communication such as signalling information, source and destination (telephone numbers, IP or MAC addresses, etc.), frequency, duration, time and date of communications. Network operators usually collect IRI for billing and network management purposes, so it is relatively easy for law enforcement agencies to gain access to this information. See 'Technical Aspects of Lawful Interception', ITU-T Technology Watch Report 6, May 2008, International Telecommunication Union, p. 3.

38. Global System for Mobile communications (GSM) and Code Division Multiple Access (CDMA) are digital cellular technologies used for transmitting mobile voice and data services.
39. Public Switched Telephone Network (PSTN) is the worldwide collection of interconnected public telephone networks that was designed primarily for voice traffic.
40. National Association of Software and Services Companies (NASSCOM) is a trade association of Indian Information Technology and Business Process Outsourcing industry.