ESPIONAGE, INTELLIGENCE AND EXPLOITATION IN THE DIGITAL AGE: CONCURRENT MANIFESTATIONS OF THE CYBER ZEITGEIST

ASHISH GUPTA

Kautilya's *Arthasastra*, composed around 321 BCE, is one of the oldest and most comprehensive treatises,[1] which still acts as a signpost and a point of reference, giving pragmatic and empirical solutions to theoreticians and practitioners, on complex statecraft issues. The exhaustive and indigenous political theory propounded by Kautilya covers many tenets of statecraft including diplomacy, peace, intelligence, security, war and political economy. According to Kautilya, *'yuddh'* or war was of three kinds: *Prakash-yuddha*, (open fight) at a place and time of choosing, *Kuta-yuddha* (concealed fighting) involving cunning and tactical manoeuvring in the battlefield, and *Tusnim-yuddha* (silent fighting) by using secret agents for enticement or neutralisation of the enemy.[2] In today's geo-political landscape, an open fight or *'Prakash-yuddha' continues to be a conceptual possibility, if not an empirical reality in all domains of war.* On the other hand, the tenets of *Kuta-yuddha* (concealed fighting) and *Tusnim-yuddha* (silent fighting), as described by Kautilya, are still visible and applicable across the

Group Captain **Ashish Gupta** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

[1] P.K.Gautam, "One Hundred Years of Kautilya's Arthasastra", *IDSA Monograph Series*, No. 20, July 2013, p.1.

[2] R.P. Kangle, *The Kautilya Arthasastra, Part 3: A Study* (Delhi: Motilal Banarsidass, 2010), p.258.

broad spectrum of strategic manoeuvring and geo-political engagement among nations. In the realm of modern warfare, the conceptual expositions as well as practical applications of Kautilya's *Kuta-yuddha* and *Tusnim-yuddha* still serve as anchoring points for strategic perception management, and intelligence and counter-intelligence operations across political, economic and military dimensions.

In the realm of modern warfare, the conceptual expositions as well as practical applications of Kautilya's *Kuta-yuddha* and *Tusnim-yuddha* still serve as anchoring points for strategic perception management, and intelligence and counter-intelligence operations across political, economic and military dimensions.

The relevance of the *Arthasastra* in the present scenario is both insightful and profound. Some of the concepts propagated by Kautilya have a parallel and undeniable resemblance with existing practices of espionage undertaken by several nation-states, either as a pretext for securing their national interests or for complying with its strategic objectives. For the advancement and achievement of the short and long-term objectives, espionage, in one form or other, has been used—deliberately, relentlessly and unrepentantly—by almost every nation-state. The practitioners of this clandestine craft undertake intelligence gathering activities across a broad spectrum of fields, construed as vital for the security, economy and military of adversaries. The professionalism and tactical value of the skills of these agent provocateurs is much sought after in peace-time and becomes almost indispensable in the times leading to, and during, a war.

The generation and processing of an unimaginable quantity of data is a manifestation of the 'cyber Zeitgeist'. For almost all agencies, organisations institutions or individuals, data from a range of sources, is a resource that can be analysed and synthesised for decision-making. Data as a resource must be protected and preserved across its life cycle. Lost and compromised data can result in financial losses, loss of confidential information and, with that, loss of credibility, functionality and operational effectiveness. The measure of criticality of data determines its ultimate importance to friends and foes alike. The efforts to protect data are matched with incentives to access, steal or manipulate information. In effect, intelligence is the product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of collected information.[3]

The systematic institutionalisation of cyber espionage and associated clandestine activities to garner, analyse and synthesise data has emerged as a new discipline or set of disciplines.

Most nations have complied with the demands of the grim imperative of cyber espionage, revamping it as an inalienable necessity and an instrument of state policy. Intelligence in its essence pertains to the ways in which sovereign powers create, exploit, and protect secret advantages against other sovereignties. Sovereignty, of course, need not be a modern state; it also comprises "non-state actors" who have the will and the means to use force to control territory, resources, and other people.[4] The systematic institutionalisation of cyber espionage and associated clandestine activities to garner, analyse and synthesise data has emerged as a new discipline or set of disciplines, combining traditional intelligence methods with new and sophisticated technical approaches.

EVOLUTION OF INFORMATION GATHERING IN CYBER SPACE

In the practice of the craft of intelligence gathering, some tools, techniques and methodologies have remained free from the political, cultural, temporal and spatial imperatives, while some have evolved into distinctively different forms, necessitated by the changed characteristics of the targets, types of information and the evolving intent. All humans are endowed with intelligence and memory along with social, emotional and cognitive vulnerabilities and are likely to unwittingly or otherwise succumb to the temptations of power, greed and ambition. The elicitation of intelligence from human sources has been used across the expanse of history. Human

[3] National Security Decision Directive 298, *The National Operations Security Program: Compendium of OPSEC Terms,* Greenbelt, MD: IOSS, (1991).

[4] Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Georgetown: Georgetown University Press, 2014), p.2.

Intelligence (HUMINT) is the most common and highly effective method used for espionage. HUMINT is defined as "a category of intelligence derived from information collected and provided by human sources."[5] Intelligence agencies have refined the art of exploiting people, using cyber space in general and the social media in particular, by intimidation, allurement or fraudulent means in garnering critical intelligence.

The intelligence gathering process involving visual clues, pictures and images collected, collated and analysed during a specific time period is an effective and result oriented methodology. For a battlefield commander, real time visual clues provide 'real time situational awareness'—the holy grail of intelligence. During the American Civil War, the Union Army used hot air balloons for observation and photography.[6] The Germans experimented with both kites and rockets as platforms in the late 1800s.[7] With the advent of flight, aerial photography became an integral part of the information and intelligence gathering processes. The evolution of some of the finest flying machines such as the Lockheed U-2, Lockheed SR-71 "Blackbird" and MiG-25 is largely attributable to the accordance of extreme relevance of, and importance given to, Imagery Intelligence (IMINT) during times of both peace and war. With satellites and Unmanned Aerial Vehicles (UAV), the aerial intelligence acquisition techniques have transformed to a new level. Basic satellite imagery can now be easily accessed by the click of a mouse using Google Maps and Google World.

In the annals of history, cryptography and espionage may have their genesis in the same time period. From a humble beginning during the Roman period, the rennaissance and resurrection of cryptography in the form of complex codes and ciphers is mainly attributable to French and Italian cryptographers in the 1500s.[8] In early 1917, the deciphering of a German encoded telegram, often referred to as the "Zimmerman Telegram",

[5] US Military Intelligence Handbook, *Strategic information, Procedure and Developments* (Washington: International Business Publications, 2011), p.249.

[6] J.K. Petersen, *Handbook of Surveillance Technologies, Third Edition* (New York: CRC Press, 2012), p.571.

[7] Ibid., p.569.

[8] Will Gragido, and John Pirc, *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats* (Burlington: Elsevier, 2011), p.111.

changed the course of the war. The "Zimmerman Telegram" was a secret communication from the Foreign Secretary of the German Empire, Arthur Zimmerman, to the German ambassador to make an offer to Mexico for it to join the German cause and, in return, to reclaim the territory of New Mexico, Texas, and Arizona from the United States. Until that point, the United States saw the war largely as a European affair and attempted to remain neutral. On being informed about the contents of the telegram, the US officially declared war against Germany and its allies on April 6, 1917. [9]

During World War II, Arthur Scherbius invented the 'Enigma', an ingenious electro-mechanical machine for encryption and decryption.[10] The Enigma had several rotors and gears which could be arranged in numerous configurations, making it virtually unbreakable with brute force methods. The claim of '*unbreakability* of encryptions' provided by Enigma made German operators over-confident about their ability to encrypt secret messages. To break the innumerable key combinations of Enigma, Alan Turing designed and used the first electronic computer which helped in "deciphering the Enigma code". The German over-confidence and over-reliance on Enigma during the course of the war was exploited to the hilt by the Allied cryptographers.[11] For code breaking or cryptanalysis, the signals or messages transiting between people (e.g. Communications Intelligence or COMINT) or between machines or networks (e.g. Electronic Communication or ELINT) or a combination of the two need to be intercepted, collated and analysed.

Cryptologic encryption has become almost a standard requirement for the privacy of electronic mail, secure-commerce transactions and the digital economy. End-to-end encryption ensures that the data in any conceivable form are encrypted in transit and in storage, and the key to decrypt these is available only with those communicating mutually. To counter these, the governments of some countries, such as the US, are trying to force the tech companies to provide 'back doors' within the encryption schemes to facilitate

[9] Thomas Boghardt, *The Zimmermann Telegram: Intelligence, Diplomacy, and America's Entry Into World War I* (Maryland: Naval Institute Press, 2012), p.31.

[10] Miloslav Dusek, Norbert Lutkenhaus and Martin Hendrych, *Quantum Cryptology Progress in Optics, Volume 49* (Amsterdam: Elsevier, 2006), p. 385.

[11] Ibid.

privileged access to the law enforcement and secret services agencies. After the San Bernardino shooting, on December 9, 2015, the Federal Bureau of Investigation (FBI) Director James B. Comey, while making a statement before the Senate Judiciary Committee, brought out that the Islamic State in Syria (ISIS) is increasingly using encrypted private messaging platforms. He said, "This real and growing gap, which the FBI refers to as 'Going Dark', we believe, it must be addressed, since the resulting risks are grave in both traditional criminal matters as well as in national security matters." He further commented that the US government is trying to ensure that the private players who own and operate these platforms – with end-to-end encryption – understand the national security risks that result from the use of their encrypted products and services by malicious actors. Though there is no legislating obligation upon these companies, the companies are being asked to cooperate constructively with the US government. [12]

RESEARCH IN OPEN PUBLICATIONS (OSINT)

The publicly accessible information, which can be scouted from a myriad sources, is a treasure trove of data capable of producing actionable intelligence. The initial scepticism about acquisition of intelligence from non-classified and open sources has given way to acceptance of this form of intelligence gathering, as a mainstay of intelligence operations. Tools and methodologies are being evolved within the national security apparatus on how to use information *gleaned from open sources.* The evolution of Open Source Intelligence (OSINT) as a mainstay of intelligence operations can be attributed to three main factors. The first is the paradigm shift in challenges from the largely state-centric security considerations of the Cold War era to the multiple threats emanating from more diverse individuals, groups or agencies. During the Cold War, the primary focus of the Western intelligence community was on the intentions and capabilities of the Soviet Union and its allies. Similarly, Soviet intelligence agencies

[12] The US Federal Bureau of Investigation, *Oversight of the Federal Bureau of Investigation, James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee* (Washington, D.C: December 9, 2015), https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8. Accessed on January 20, 2016.

were actively involved in intelligence gathering about their adversaries. The disintegration of the erstwhile USSR, emergence of a new world order and evolution of contemporary terrorism in a more dangerous and deadlier form, have given rise to many challenges for the intelligence community. The scope and range of issues to be dealt with by the intelligence agencies have spiralled to unprecedented levels. Terrorism, organised crime, state sponsored terrorism, home-grown terrorist organisations, proliferation of illegal weapons, rogue states, illegal immigration and energy security are the issues that keep the intelligence agencies on their toes at all times. In the wake of multifarious challenges to national security and the widening of the security agenda to non-military threats, intelligence agencies have to trawl through gathered intelligence to identify subtle and specific signatures to determine the magnitude, timing and place of conditioned responses**.** This, in turn, has seen a greater demand for more information and a natural progression of this is the increased reliance and utilisation of OSINT. A second driver for the growth of OSNIT is technology. The emergence of the collaborative web and the presence of the ubiquitous internet have provided the security actors a new set of tools and technologies for collecting, collating, analysing, and disseminating information in a very short time.

WEB SOURCE INTELLIGENCE (WEBINT)

The ability to gather information by leveraging the power of the internet is termed as WEBINT. By using powerful web crawlers and indexing systems, it is possible to harvest just about any piece of information stored on publicly available servers. The incentives to undertake acts of cyber crime, espionage, subversion and sabotage are only limited by the ingenuity, dexterity and technological capabilities possessed by hostile malevolent entities. The successful culmination of an espionage activity in cyber space may be a technology and capability demonstrator, a deliberate attempt to garner tangible and intangible results or a premediated design to cause severe *disruption* in the *functioning* of political, financial, social or military entities. An act of espionage in cyber space by a state may also be a manifestation of its deterrence capability. After all, credible deterrence depends on communication of actions and responses in the wake of the adversaries' attempts to cross the security threshold prescribed by the state in pursuant to its stated national interests.

The cyber attackers have become more ingenious and opportunistic in their endeavours, and attack vectors and techniques have evolved in terms of lethality and consequences.

CYBER ESPIONAGE AND EXPLOITATION

Today, use of stealth techniques and exploits with an aim to exploit the computers and networks of various organisations and institutions, has become a menace of unparalleled proportions. Cyber crime and espionage reveal the dark underbelly of cyber space. This has given rise to an increasingly dangerous ecosystem inextricably embedded within the fabric of global cyber space. This ecosystem is teeming with inimical activities and devious enterprises, not only within existing precincts but foraying in systems beyond immediate reach. The cyber attackers have become more ingenious and opportunistic in their endeavours, and attack vectors and techniques have evolved in terms of lethality and consequences. The cyber espionage activities may also be undertaken to keep the dynamic relationship equation consistent between two rival states. The desire of a state to bring parity to the sum total of all capabilities may be the main motivation for the adoption of non-conventional means. The dedicated cyber espionage campaigns launched by China against the US may be one of the drivers for this. China tries to make up for what it lacks in conventional military means by exploiting the cyber space.

Cyber espionage activities may provoke a reaction and intensify latent hostilities. The reaction can be offensive or defensive in nature, based on the perceived tolerance threshold. Defensive actions in response to an espionage activity are generally exhaustive and, at times, are way out of proportion in terms of resources, time and manpower. In a bid to secure itself from future cyber espionage threats, the target may over-react and over-protect. In the bargain, it may lose out on opportunities the global information age has to offer. This sets in motion a vicious circle in which a substantial amount of money is committed to clean up existing systems malware while even more money is spent for future protection. This may end up being a *'Pyrrhic victory'* as the time, money and efforts spent may not result in accruing the intended results.

CYBER ESPIONAGE BY NON-STATE ACTORS

Although nation-states tend to have larger stakes in exploitation of cyber space, non-state actors have equal motivation, though for different reasons. The use of cyber space as a potential venue for undertaking various malevolent, insidious and treacherous activities has become the order of the day. While motives may vary from one hacker to the next, the objective is consistent with the goal of exploiting the cyber space for malicious intents. Financial gains, espionage, ephemeral fame, nefarious notoriety, entertainment, hacktivism, terrorism or misplaced sense of patriotism are some of the drivers which propel hackers into the murky world of cyber crime. Motivation for making money rules the roost, closely followed by corporate espionage activities. The hacking skills acquired by individuals are much sought after and there is an increasing demand for their services for industrial espionage, *intellectual property thefts*, financial frauds and monetary misappropriation.

Cyber criminals and cyber espionage operators have evolved a myriad attack techniques with ever-increasing lethality and sophistication commensurate with their evolving expertise and experience.

Cyber criminals and cyber espionage operators have evolved a myriad attack techniques with ever-increasing lethality and sophistication commensurate with their evolving expertise and experience. A cyber criminal gains currency in a small, exclusive and secretive community, based on the success, quantum and frequency of his exploits. The success of such exploits largely depends on the understanding of the system architecture, network transmission protocols, exploitation of associated vulnerabilities, malicious codes and content exploits. The understanding of almost every aspect of human fallibility and frailty also assists them in their nefarious endeavours.

ZERO DAY VULNERABILITY EXPLOITATION

In recent times, the vulnerability quotient due to espionage activities in cyber space has gone up many notches. A direct ramification of this is a burgeoning market offering services, tools and technologies facilitating credible and potent espionage activities. The spirit of entrepreneurship has caught up with computer geeks, who have the proven prowess in exploiting cyber vulnerabilities, and no qualms in offering their services to the highest bidder. These espionage activities in cyber space may threaten the economy and national security and well-being of people.

The mother of all malicious programmes and bugs is the "zero day exploit". In a zero day exploit, the creation of the exploit is concomitant with the knowledge of vulnerability before, or on the same day. By creating a virus or bug that takes advantage of a vulnerability not known to the vendor and without a security patch, the attacker can inflict debilitating damage on unsuspecting victims. On an average, zero day vulnerability remains unknown to the affected software vendor and its users for an average of 312 days. [13]

In the recent past, software vendors and security researchers have been caught up in an animated debate on the issue of ethicality, legality and desirability of disclosing vulnerability information. The dichotomous dilemma of making the information public, on the one hand, may allow all the affected parties to carry out risk assessment while, on the other, the information will also be available for exploitation. The dependence of society on information technology has transformed the knowledge about security vulnerabilities, a highly prized and valuable asset. An ethical security researcher may seek monetary compensation for the time spent uncovering vulnerabilities. However, reporting vulnerabilities for seeking compensation might be viewed as akin to extortion by the vendor. On the other hand, cyber criminals, with no ethical considerations, are willing to pay a substantial amount for suitable vulnerability information. The market for sale and purchase of vulnerabilities has evolved from its nascent stage,

[13] Krebsonsecurity, "How Many Zero Days Hit You Today? ", http://krebsonsecurity.com/2013/12/how-many-zero-days-hit-you-today/. Accessed on May 1, 2016.

operating from dark and isolated alleys under the shroud of anonymity, to commercial service offerings with legitimacy.

Vulnerability Purchase Programmes

Traditionally, the primary players in the commercial vulnerability market have been iDefense, which started its Vulnerability Contributor Programme (VCP)[14] in 2002 and TippingPoint, which started its Zero Day Initiative (ZDI)[15] in 2005. In a bid to show their ethical intents, both vendors publicly disclosed their vulnerability handling services and policies. The VCP and ZDI programmes typically purchase vulnerability information to protect customers before the vulnerability becomes public knowledge, subsequently informing the vendor of the affected software. The VCP and ZDI programmes entreat security researchers to accept lower compensation with the assurance that the information would not be used with malicious intent. Upon acquiring a vulnerability, both programmes provide detailed technical information on the vulnerability and on the timeline from its initial purchase through publication. Under the VCP and ZDI programmes, the two companies together had purchased 2,392 vulnerabilities till September 23, 2013.

Bug Bounty Programmes

In order to bring in resilience to their products, a number of software vendors have embarked on 'Bug Bounty Programmes'. Under this programme, a finder can directly report a vulnerability to the software vendor and is monetarily compensated by the vendor. This incentive may discourage a finder going public with the vulnerability information or selling it to an unscrupulous person. It was first introduced by the Mozilla Foundation and since then, Google, Facebook, PayPal and others have followed suit. Microsoft, which vehemently opposed such a system, finally succumbed to commercial and security imperatives and introduced its bug bounty programme.

[14] "VeriSign iDefense Threat Intelligence Services Overview", https:// www. verisign.com /static / 031415.pdf. Accessed on May 1, 2016.

[15] "Why Did We Create the Zero Day Initiative?", http://www.zerodayinitiative.com/about/. Accessed on May 1, 2016.

- Under the bug bounty programme, Google, on January 28, 2016, announced that it had paid more than US $ 2 million to security researchers in the year 2015. Since the launch of the programme in 2010, the company had paid more than US $ 6 million, with the largest single payment of US $ 37,500 to an Android security researcher. [16]
- Mozilla, in the last three years, has paid approximately US $ 570,00 for the knowledge of 190 vulnerabilities which were discovered in the Firefox browser.
- Facebook has paid out a whopping US $ 4.3 million since it introduced its bug bounty programme in 2011 to more than 800 researchers around the world.[17]
- Microsoft has paid to the tune of US $ 100,000 from June 2013 onwards, when it decided to became part of the bug bounty programme. On October 8, 2013, it awarded US $ 100,000 to James Forshaw (the head of vulnerability research at Context Information Security) for discovering a new type of mitigation bypass technique that could potentially threaten the security and integrity of its latest version of Windows operating system.[18]

The cost benefit accrued by the bug bounty programme is much higher than the cost of hiring full-time security researchers to locate bugs internally. Bug bounty programmes help software vendors to plug in the security loopholes which otherwise have the potential to be exploited offensively. It also hastens the action towards remedy of vulnerabilities reported through a bug bounty programme.

Most nation-states are leveraging cyber warfare techniques either with hostile intent or for the protection of their Critical Information Infrastructure (CII). In the recent past, the budget outlays and spending to acquire capabilities

[16] Google Security Rewards - 2015 Year in Review, "Google Security Blog", https://security.googleblog.com/ 2016/01/google-security-rewards-2015-year-in.html. Accessed on May 1, 2016.

[17] "2015 Highlights: Less Low-Hanging Fruit," Facebook Bug Bounty, https://www.facebook.com/BugBounty/. Accessed on May 1, 2016.

[18] "Microsoft-Pay-Out-First-100000-Bug-Bounty", available on http://nakedsecurity.sophos.com/2013/10/09. Accessed on May 1, 2016.

for waging cyber war have increased manifold. While unethical hackers and even criminal organisations have limited resources and have to operate within the confines of shoe-string budgets, a nation-state's cyber warfare assets have plenteous resources and immunity from prosecution. In order to stay a step ahead of potential adversaries, it is not uncommon for nation-states to purchase vulnerabilities for exploitation. The US government, for example, is an enthusiastic buyer, with the National Security Agency (NSA) devoting US $ 25.1 million to "covert purchases of software vulnerabilities" from private vendors during the fiscal year 2013. This would enable it to acquire an estimated minimum of 100 to 625 exploits based on the present going rate.[19] Other countries are also big spenders when it comes to acquiring exploits.

The year 2009 was a defining year which marked the arrival of the first true cyber weapon, the "Stuxnet'. A complex computer worm was developed with the specific objective to decommission uranium enrichment facilities in Natanz in Iran. It is believed that the perpetrators used four zero day security vulnerabilities to spread around Microsoft's Windows operating system. After detailed study, Microsoft admitted that the attackers initially exploited the old MS08-067 vulnerability which was a remote code execution vulnerability. Successful exploitation of this vulnerability enables the attacker to take complete control of an affected system remotely.[20] A new LNK (Windows Shortcut) flaw was used to launch the exploit code on vulnerable Windows systems and a zero day bug to exploit the print spooler vulnerability (this vulnerability was leveraged to propagate and affect systems connected to the affected machine's network).

Presently, a number of new entrants are offering services ranging from vulnerability feed, penetration testing to vulnerability and security assessment. Among them are Exodus Intelligence and Netragard in the US, Vupen in France, Revuln in Malta and Telus in Canada. In fact, Vupen openly offers sales of "exclusive and extremely sophisticated zero days

[19] Stefan Frei, "The Known Unknowns : Empirical Analysis of Publicly Unknown Security Vulnerabilities", NSS Labs, p.14.

[20] "Vulnerability in Server Service Could Allow Remote Code Execution", http://support. microsoft.com /kb/958644 MS08-067. Accessed on May 1, 2016.

for offensive security". It also advertises that it offers government-grade zero day exploits which could be used by law enforcement agencies and the intelligence community in furtherance of their offensive cyber missions and operations. These companies are hunting with the hounds and running with the hares with an aim to make money by leveraging the fear factor emanating from concerns among companies and organisations about the security of their systems as well as by selling the zero day exploits to the highest bidder.

Big software vendors will leave no stone unturned to plug these vulnerabilities either by internal evaluation or by purchase from vendors under the bug bounty programme.

On any given day, a number of vulnerabilities are privately known. Out of these, it can be safely assumed that a substantial number are exploitable. These vulnerabilities and exploits are being purchased with equal gusto by cyber criminals as well as by government agencies. Big software vendors will leave no stone unturned to plug these vulnerabilities either by internal evaluation or by purchase from vendors under the bug bounty programme. This has added a new dimension to an already complex issue of cyber espionage and exploitation.

LARGE-SCALE SURVEILLANCE PROGRAMMES

The *governments of some of powerful nations*, such as the US and China have embarked on an organised, state sponsored but publicly denied surveillance programme, in effect, *trampling 'the human right of privacy' with impunity.* Such acts often lead to a dichotomy between the government's overt assertion of human rights and covert sponsoring of mass surveillance on its own citizens.

US Surveillance State

In one of the earlier such attempts, under the US-UK Security Agreement, the five signatory nations namely, Australia, Canada, New Zealand, the UK and the US became part of the Signals Intelligence (SIGINT) collection and analysis network, code-named "Echelon". With the objective of monitoring the communications of the erstwhile USSR and its allies in the 1960s, the Echelon carried out interception and eavesdropping on voice and data communication over commercial satellites. With the arrival of the ubiquitous internet, the electronic communication was largely being transmitted through this new medium. In order to monitor the traffic going to and from a suspicious target, in the late 1990s, the US FBI came up with the "Carnivore" programme. The fruition of the programme saw the attachment of a device at the Internet Service Provider (ISP) of the target facilitating filtering and recording of all inbound and outbound traffic.[21] Under much public outcry, the programme was abandoned in 2001, only to metamorphose into commercially available devices. Still trying to make strides in the field of mass surveillance,[22] the FBI developed the "Magic Lantern" technology which allowed installation of powerful software on a remote machine, transmitted through an exploit or a Trojan horse via a seemingly innocuous yet extremely malicious e-mail.[23] Once installed, the software would begin to record every keystroke made on the compromised machine. In the year 2002, the existence of the Magic Lantern programme was confirmed by the FBI, however, with the equally implausible statement of denial of its deployment ever.

In the year 2002, the existence of the Magic Lantern programme was confirmed by the FBI, however, with the equally implausible statement of denial of its deployment ever.

Tone and Tenor of Mass Surveillance after 9/11

The American psyche, lacerated with hurt, clouded with anger and ripe with distrust, scepticism, alienation and self-criticism in the aftermath of the September 11 attacks in 2001, was malleable to the acceptance of

[21] Talitha Nabbali, and Mark Perry. "Going for the Throat: Carnivore in an Echelon World—Part I." *Computer Law & Security Review* 19.6, 2003, pp. 456-467.

[22] Ted Bridis , "FBI Develops Eavesdropping Tools", Centre for Research on Globalisation (CRG), November 23, 2001, http://globalresearch.ca/articles/BRI111A.html._Accessed on April 23, 2016.

[23] Ibid.

some harsh steps. The resolve to negate the possibility of future attacks of such magnitude paved the way for the enactment of many laws granting sweeping powers to government agencies to undertake mass surveillance such as the Patriot Act, Protect America Act and FISA (Foreign Surveillance Act) Amendments Act. Under the Protect America Act, the mandatory requirement of a warrant for government surveillance of foreign targets was removed.[24] Under the FISA Amendments Act, some of the original FISA court requirements were dispensed with.[25] The US National Security Agency (NSA) and its international collaborative partners went into overdrive to bring every US citizen and all possible foreign nationals, even without any significant interest in US affairs, under the surveillance net. However, some in investigative journalism got wind of what the government agencies were up to. In November 2010, WikiLeaks and five major news journals, namely, *El Paí*s of Spain, *Le Monde* of France, *Der Spiegel* of Germany, *The Guardian* of the United Kingdom and *The New York Times* of the United States began publishing leaked US State Department diplomatic "cables" simultaneously.[26] Other documents of classified nature which were leaked to the public domain included the Afghan War documents, Iraq War documents and the Guantanamo Bay files leak. However, to witness the mother of all leaks, the world had to wait till June 6, 2013, when the British newspaper *The Guardian* began publishing a series of revelations made available by Edward Snowden, an ex-NSA-contracted systems analyst. Snowden, acting as a whistleblower, came in contact with two journalists, Glenn Greenwald and Laura Poitras, and provided them a cache of around

[24] 107th Congress (2001-2002), "H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001", https://www.congress .gov/bill/107th-congress/ house-bill/3162. Accessed on April 23, 2016.

[25] 110th Congress (2007-2008), "H.R.3773 - FISA Amendments Act of 2008", https:// www.congress. gov/bill/110th-congress/house-bill/3773?q=%7B%22search%22%3A %5B%22FISA+Amendments +Act%22%5D%7D&resultIndex=1. Accessed on April 23, 2016.

[26] Nick Davies, "Afghanistan War Logs: Story Behind Biggest Leak in Intelligence History", *The Guardian*, July 25, 2010, http://www.theguardian.com/world/2010/jul/25/wikileaks-war-logs-back-story. Accessed on April 23, 2016.

15,000–20,000 documents.[27] The Snowden revelations made it amply clear that the NSA was operating a complex and intricate network of spying programmes intercepting internet and telephone conversations from over a billion users around the world.

Snowden's act was criticised and applauded in equal measure from various quarters. NSA Director General Keith Alexander in a swift and acerbic statement blamed Snowden for causing "irreversible damage" to the US.[28] The Senate Intelligence Committee Chair Dianne Feinstein described Snowden's action as treasonous. The process to indict Snowden on charges of espionage and treason was initiated. However, some saw the situation from a different vantage point. Former Vice President Al Gore viewed the NSA surveillance as violation of the Fourth Amendment (Amendment IV) to the United States Constitution.[29]

The Snowden revelations have triggered a dichotomous debate over the issue of accountability and the value of privacy. There is a perceptible shift in opinion in many parts of the world over not succumbing to the "*Orwellian doublespeak*" of the high and mighty. Besides, there is a resurgence of resolve and renewed vigour among mainstream media to sensitise the public on key issues that may have been deliberately kept out of the public domain. However, the Snowden disclosures have not firmed up the resolve of an overwhelming majority of countries to respond in any tangible measure. If we look closely and dissect through the layers of protests in the form of representations, governmental inquiries and media coverage, the collective measures for prevention and mitigation of such occurrences were largely insignificant. The small numbers of reforms that have been adopted by governments appear to lack the necessary drive to set up an institutionalised

[27] Glenn Greenwald, Ewen MacAskill and Laura Poitras , "Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations", *The Guardian*, June 11, 2013, http://www.theguardian.com/world/2013/jun/09/ edward- snowden -nsa-whistleblower-surveillance. Accessed on April 23, 2016.

[28] Spencer Ackerman and Dominic Rushe , "NSA Director: Edward Snowden has Caused Irreversible Damage to US", *The Guardian*, June 17, 2013http://www.theguardian.com/world/2013/jun/23/nsa-director-snowden-hong-kong. Accessed on April 23, 2016.

[29] Suzanne Goldenberg, "Al Gore: NSA's Secret Surveillance Program 'Not Really the American Way' ", *The Guardian*, June 14, 2013, http://www.theguardian.com/world/2013/jun/14/al-gore-nsa-surveillance-unamerican. Accessed on April 23, 2016.

international system with provisions for prosecution and punitive actions to act as deterrence.

China's Quest for Mass Surveillance

The Communist Party of China, while being weary of the implications of the legitimacy of its unrestricted online access to information, has enthusiastically promoted the use of the internet as an inalienable part of its quest for global hegemony, economic growth and orchestration of its technical prowess. China views the internet as a fertile ecosystem that germinates, fosters, nurtures, and engenders political dissent, detrimental social activities and societal unrests. To counter this, China has an aggressive and multi-faceted online censorship system, commonly known as the Great Firewall. After viewing the contents on the internet through the prism of its own contentious policies and cultural interests, the censorship apparatus filters or blocks access to online material deemed dangerous to the state.

The Chinese leadership has, for long, had an ambivalent relationship with the internet. During the Arab Spring in early 2011, China bolstered its censorship bureaucracy, reportedly creating a new office under the State Council Information Office to "regulate every corner of the nation's vast internet community,"[30] However, confinement within the precinct of the Great Firewall has given an impetus to an evolving and thriving Chinese online ecosystem, *driven, sustained and perpetuated by indigenous innovation*, *enterprise and entrepreneurship.* Beijing's efforts to alienate its citizens from the global net has paved the way for home-grown companies to cater to the online requirements and needs of 1.3 billion people in their societal interactions, financial transactions, knowledge exploration, online resource exploitation and a myriad other services. The internet's ubiquitous and totemic icons—Google, Wikipedia, Twitter, YouTube, Facebook, Instagram — are under the censorship of the ruling Communist Party due to the fears of fanning the flames of anti-government sentiments. In the absence of a competitive environment, Chinese home grown companies are thriving and

[30] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Serach of Cyber Peace* (New York: Cambridge University Press, 2014).

have garnered market *capitalisation*, even exceeding that of their foreign counterparts whom they emulate.

At the helm of the Chinese online oppression against free speech and tyrannical censorship is China's new internet czar Lu Wei who took over the State Internet Information Office in 2013 and became the director of a powerful Internet Committee headed by President Xi Jinping in 2014.[31] While unrepentantly defending China's need for stronger internet content control, he has issued new regulations restricting sharing on social media sites and increasing censorship of popular online video sites. In a response over such controls, Lu Wei said "The internet is like a car. If it has no brakes, it doesn't matter how fast the car is capable of traveling, once it gets on the highway you can imagine what the end result will be." [32]

The home-grown Chinese firms have ensured that most of the Chinese incarcerated behind the Great Firewall are not deprived of online experiences and services unless they want to voice their political dissent online. Adherence to Chinese government regulations and sticking to Chinese sites is rewarded with sufficiently high speeds and reasonable access charges. In the first quarter of 2015, the total transaction value of China's e-commerce market exceeded US$ 567.49 billion, an increase of 10.1 percent on a *year-over-year* basis.[33] As of December 31, 2014, the top five listed Chinese internet companies by market value were Alibaba (US $253.41 billion), Tencent (US$135.50 billion), Baidu (US$80.32 billion), Jingdong (US$31.52 billion) and Netease (US $ 13.01 billion). In September last year, e-commerce king Alibaba scored the largest Initial Public Offer (IPO) in Wall Street history. Tencent, the designer of the messaging company WeChat, has a market capital more than that of IBM. As a hybrid of Twitter and Facebook, Sina Weibo has emerged as the most popular Chinese microblogging website with a market penetration comparable to that of Twitter.

[31] Paul Mozur and Jane Perlez, "Gregarious and Direct: China's Web Doorkeeper," *New York Times*, December 2, 2014, http://www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper. html?_r=0. Accessed on July 21, 2015.

[32] David Bandurski "Lu Wei: The Internet Must Have Brakes," *China Media Project*, November 11, 2014, at http://cmp.hku.hk/2014/09/11/36011/ Lu Wei: the internet must have brakes. Accessed on July 21, 2015.

[33] Cecilia,"China E-commerce Market in Q1 2015," *China Internet Watch*, July 16, 2015, at http://www.chinainternetwatch.com/13430/e-commerce-marketq1-2015/. Accessed on April 21, 2016.

The Chinese internet strategy, aimed at containing the simmering political dissent, has a much more sinister dimension to it.

In its infancy, the internet shook the very foundation of sovereignty as propagated by the dominant 'Westphalian conceptions'. The belief that the internet's *transcendence* of physical boundaries would render it immune to *oppressive regulatory regimes* has given way to acceptance of the fact that a determined state with technical underpinnings can regulate and control the internet. The Chinese internet strategy, aimed at containing the simmering political dissent, has a much more sinister dimension to it. Chinese state-backed hackers have been accused of cyber espionage. A recent report made public by Fireeye Labs, a company that provides cyber security solutions, examination of malware aimed predominantly at entities in Southeast Asia and India, revealed a decade-long operation focussed on targets—government and commercial—that hold key political, economic and military information about the region. The planned development efforts aimed at regional targets and missions made the lab believe that this activity was state sponsored—most likely by the Chinese government.[34]

China is also determined to extend its oppressive regime beyond its borders. In the cyber lexicon repository, the term "Great Cannon" has been added alongside "Great Firewall", christening a new tool for censorship developed by China. When used offensively, this ability can turn a normal internet user into a vector of attack. In one such case, the Great Cannon intercepted traffic sent to Baidu infrastructure servers returned a malicious script, unwittingly enlisting the web surfer in the hacking campaign against foreign websites that have helped the circumventing of the Chinese censorship.[35]

[34] Fireeye Labs. "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation: How a Cyber Threat Group Exploited Governments and Commercial Entities across Southeast Asia and India for over a Decade", https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf. Accessed on April 21, 2016.

[35] Alex Hern, "'Great Cannon of China' Turns Internet Users into Weapon of Cyberwar," *The Guardian*, April 13, 2015 at http://www.theguardian.com/technology/2015/apr/13/great-cannon-china- internet-users- weapon-cyberwar. Accessed on April 21, 2016.

CONCLUSION

In the context of cyber espionage and surveillance, the mission preparedness and befitting response depend on 'early warning' of potential malevolent events and the 'motivation and resources' of an adversary. For the process to be meaningful and result oriented, it is imperative to have situation specific and contextual knowledge, discerning disposition and homogenised actions. The information and intelligence garnered through the infrastructure of surveillance and communication systems that support effective decision-making is a culmination of training efforts, experience and technical sophistication. These qualities, either acquired through training or accumulated with experience, coupled with intuitive ingenuity and intuitional perceptions, make surveillance in cyber space a widely used and useful construct.

Its scope, magnitude and implications are limited only by the ingenuity and intent of the perpetrators and the technological advancement.

The constant evolution of cyber threats is a cold hard reality which will continue to cause cataclysmic upheavals in the cyber landscape. Its scope, magnitude and implications are limited only by the ingenuity and intent of the perpetrators and the technological advancement. The most traditional information security programmes are repeatedly circumvented with impunity. Nations around the world are in a race to develop, consolidate and refine cyber warfare capabilities. To mitigate the associated risks, organisations need to evolve their current surveillance capabilities and augment these with positional and temporal accuracies by using technological innovations with persistent reconnaissance to produce timely and actionable intelligence.