CYBER ASTUTENESS: AN ELUSIVE ENABLER OF MILITARY DOMINANCE

ASHEESH SHRIVASTAVA

Operations Orchard, Estonia, Stuxnet or Black Energy have demonstrated the power of cyber space to shift the theatre of war from conventional battlefields to the 'virtual' domain. Hence, traditional physical boundaries and preventive measures are no longer relevant.

Recent world events have demonstrated increased exploitation of cyber space as a force multiplier for conventional warfare. This new method of war requires relatively fewer but highly specialised resources to mount an offensive. The techniques of cyber attacks have also specialised over the years. While traditional weaponry retains its advantages in the conventional battlefield, a cyber attack can now inflict an equally serious dent on a country's centres of gravity and critical infrastructure without physical intrusion into the adversary's air space. Cyber attacks are cheaper, more effective and easier to launch than conventional weapons and it is easier to hide the identity of those who launch them. Statistics on threats of cyber attacks also echo a paradigm shift from the relatively innocuous emails-based threats of yesteryears to more malicious threats today. Concurrently, there is also a direct cause-effect relationship between the growth of Information and Communication Technology (ICT) devices and their vulnerability to illicit and malicious cyber attacks.

Attacks or crimes in cyber space are not limited by geographical boundaries. The scale of such crimes in the recent past has made governments

Wing Commander **Asheesh Shrivastava** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

Cyber attacks are also cheaper, more effective and easier to launch than conventional weapons and it is easier to hide the identity of those who launch them. Statistics on threats of cyber attacks also echo a paradigm shift from the relatively innocuous emails-based threats of yesteryears to more malicious threats today.

take notice of the disruption these attacks cause. Moreover, the size of the economy or the military might of a nation does not necessarily reflect the nation's ability to fight a cyber attack or the *cyber security awareness* of its population. Simultaneously, cyber security is a dynamically evolving environment wherein policies, laws, organisations skill sets, mutual cooperation and technical interconnectivity of networks need to be continuously updated to ensure safety against cyber attacks. Therefore, a robust cyber ecosystem, encompassing all facets of cyber space, is required to be in place to reduce the threat to, and enhance confidence towards, increased use of ICTs. This is required to enable the rapid economic growth of a nation.

Nonetheless, in this dynamically evolving environment, only having a defensive cyber ecosystem is insufficient to guarantee safety. Therefore, on the one hand, cyber security policies have to be harmonised as well as enforced across the entire nation and, on the other, offensive capabilities also have to be articulated for added paybacks. *This article debates the advantages of offensive cyber capabilities as a force multiplier for collective defence.*

The commentary reasons for the creation of a cyber offensive force to operate in conjunction with the existing security apparatus. To justify this argument, this narrative maps the history of cyber attacks across the globe which had military annotations. From these examples, it is evident that nations use the services of non-state actors to leverage their own political or military agenda. Non-state actors are much more difficult to identify. Therefore, it is necessary to establish a robust defence ecosystem to prevent cyber attacks. The strength of the ecosystem is measured by its Global Cyber Security Index. The limitations of the measurement technique

are also discussed in the article. Thereafter, it debates how nations can strengthen their cyber ecosystem by civilian-military participation. The article recommends the adoption of a two-pronged strategy towards cyber security. Firstly, strengthening the defensive mechanism and thereafter, developing offensive capability.

The Israelis somehow took over the computer system controlling the AD radar network, resulting in the radars continuously feeding false pictures of the air space on the display monitors and making the Syrian controllers believe that all was well. The Israeli aircraft flew almost 350 km into the Syrian air space, destroyed the targets and returned safely.

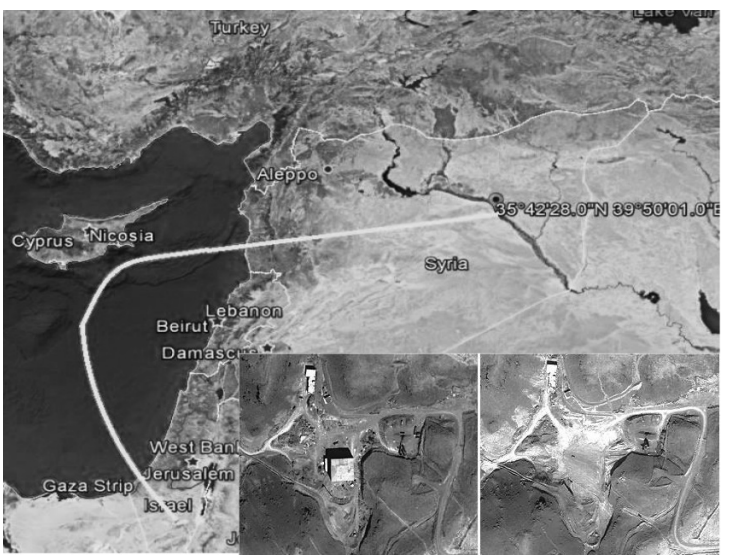
HISTORY OF KNOWN CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Recent history is replete with examples of cyber space being used to attack the critical infrastructures of adversaries, which were considered sensitive by the host nation. Cyber attacks have also been initiated by non-state actors with the candid support of state actors to alter the opinion of the populace; some examples are discussed in the following paragraphs.

Syria, September 6, 2007: The Israeli Air Force struck down a supposedly under construction nuclear reactor at Al Kibar in the Deirez-Zor region of Syria just after midnight (local time). This was called **Operation Orchard** which, according to news reports, was carried out by eight aircraft of the Israeli Air Force, including F-15s, F-16s, and Electronic Intelligence (ELINT) aircraft. The fighters were equipped with AGM-65 Maverick missiles, 500 lb bombs, and external fuel tanks. On the ground, the Israeli Air Force was assisted by a team of elite Israeli Shaldag/ Sayeret Matkal special forces commandos who painted the target with laser designators. A Google map depicting the location of the nuclear reactor and the supposed flight path of the Israeli Air Force aircraft is shown in Fig 1. The movement of the aircraft went unnoticed by the Syrian Air Defence (AD) network. It is believed that the Israeli Air Force's Electronic Warfare

(EW) system compromised the entire Syrian air defence radar system. In the event, the Israelis somehow took over the computer system controlling the Air Defence (AD) radar network, resulting in the radars continuously feeding false pictures of the air space on the display monitors and making the Syrian controllers believe that all was well. The Israeli aircraft flew almost 350 km into the Syrian air space, destroyed the targets and returned safely. The only clue of the Israeli Air Force's involvement in the mission was the sighting of an unmarked drop tank off the shores of Turkey. Later, US Air Force officials speculated that Israel used a technology similar to Suter to thwart the Syrian radars and sneak into their air space undetected during Operation Orchard. The Suter military computer programme was developed by BAE Systems for the US Air Force. It was designed to attack computer networks and communication systems of Russian origin. This event, for the first time, publicly demonstrated the offensive capabilities and reach of cyber technology as a military tool.

Fig 1: The Flight Path of Israeli Air Force Aircraft and Photos of the Target before and after the Attack



Estonia, 2007: Ethical hackers unleashed a wave of cyber attacks on Estonia, which is one of Europe's most wired countries. These Denial of Service (DoS) attacks that crippled dozens of government and corporate servers across the country are believed to have originated from Russia (refer Fig 2), a charge Moscow denies. The online assault started due to Estonia's decision to relocate a Soviet World War II memorial from downtown Tallinn, sparking off riots by the ethnic Russian minority. Experts confirmed the use of thousands of computers in a coordinated attack against government agencies and banks. A Google map screen shot showing the location of countries is placed in Fig 2.

Fig 2: Moscow DoS Attacks on Estonia

Consequences: The attacks had far-reaching consequences in Estonia and beyond, which:

- Prompted the North Atlantic Treaty Organisation (NATO) to enhance its cyber warfare capabilities and establish its cyber defence research centre at Tallinn.
- Motivated Estonia to call on the European Union to make cyber attacks a criminal offence.
- Provoked the Federal Bureau of Investigation (FBI) to position a computer crime expert in Estonia to help fight international threats against computer espionage.

The Stuxnet worm was a watershed moment in the history of cyber security and some experts even consider it as the most sophisticated malware attack ever disclosed publicly. It is believed to have been covertly developed by the Israeli Intelligence Corps Unit 8200 with patronage from the US' CIA.

- Compelled NATO's Cooperative Cyber Defence Centre of Excellence to convene an international assembly of legal scholars and practitioners to draft a manual (Tallinn Manual[1]) to address issues on how to interpret international criminal laws in the context of cyber operations, cyber warfare and cyber offences.

Iran, June 2010: Iranian officials discovered that the computers of the control system unit at one of its nuclear (uranium) processing/enrichment plant had been infected by a computer worm called Stuxnet[2]. This worm had a masterful and malicious piece of code that attacked in three phases. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. It then hunted for Siemens Step7 software, which was also Windows-based and used to programme industrial control systems operating equipment such as the centrifuges of the nuclear plant. Lastly, it compromised the Programmable Logic Controllers (PLC). As a result, the worm disrupted the industrial systems and caused the centrifuges to spin uncontrollably and shut down the plant. The worm was specifically programmed to target the Supervisory Control and Data Acquisition (SCADA)[3] systems that were used to monitor and control centrifuges at Iran's nuclear enrichment plant at Natanz[4].

1. The Tallinn Manual 1.0 (originally Tallinn Manual on the International Law Applicable to Cyber Warfare) is an academic, non-binding study on how international law (in particular, the Jus ad Bellum and International Humanitarian Law) applies to cyber conflicts and cyber warfare.
2. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *The Wired*, March 11, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. Accessed on July 17, 2017
3. SCADA (Supervisory Control and Data Acquisition) is a computer based industrial automation control system that practically makes factories and utilities run on their own. In an electrical system, SCADA maintains a balance between demand and supply in the grid and increasing its efficiency.
4. David Kushner, "The Real Story of Stuxnet: How Malware was Detected", *IEEE Spectrum*, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed on July 17, 2017

The Stuxnet worm was a watershed moment in the history of cyber security and some experts even consider it as the most sophisticated malware attack ever disclosed publicly. It is believed to have been covertly developed by the Israeli Intelligence Corps Unit 8200 with patronage from the US' Central Intelligence Agency (CIA)[5].

Ukraine, December 23, 2015: Thirty power sub-stations distributing electricity to thousands of domestic consumers in central Ukraine were remotely disconnected from the national power grid. This attack on the power grid was codenamed Operation Black Energy[6] by the US authorities. Although the outage lasted for only about 2-8 hours, the hacking demonstrated the capabilities of cyber experts to remotely take over the SCADA systems. The adversaries entered the SCADA networks through hijacked Virtual Private Networks (VPNs) and sent commands to disable the Uninterrupted Power Supply (UPS) systems they had already reconfigured. Thereafter, they began to switch-off circuit breakers one by one, disconnecting the local sub-stations from the national power grid. Concurrently, they also launched a telephone denial-of-service attack against customer call centres to prevent customers from calling-in to report the outage. This gave the attackers more time to complete their mission and prevented the power distribution companies from becoming aware of the ground situation and the scale of the failure. This move illustrated a high level of sophistication and planning on the part of the attackers.

Ukraine has claimed with certainty that Russia was behind the attack, as relations between Russia and Ukraine had been strained ever since Russia annexed Crimea in 2014 and Crimean authorities began nationalising Ukrainian-owned power generation companies located within Crimea. Much before the December blackout in Ukraine, pro-Ukrainian activists had physically attacked a few sub-stations feeding power to Crimea, leaving about two million Crimean residents without power for over a day. Therefore, it

5. Richard Behar, "Inside Israel's Secret Startup Machine", *Forbes Magazine*, May 11, 2016, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#50b1b2691a51. Accessed on July 17, 2017.
6. Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack", *The Wired,* January 20, 2016, https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. Accessed on July 24, 2017.

was speculated that this blackout in Ukraine was a retaliatory cyber attack by the Russians to avenge the Crimean blackout.

These examples are just a few of the many cyber attacks launched every day by state and non-state actors against public/ private establishments. On many occasions, these assaults go undetected due to the lack of awareness of the users or losses not being attributed to cyber attacks. With time, the technology and complexity of the attacks are increasing progressively. This is making concealment easier and proving culpability almost impossible. Notwithstanding, the distinguishing characteristics of cyber attacks vis-à-vis conventional warfare have, by and large, remained unaltered over time.

CHARACTERISTICS OF A CYBER ATTACK

A cyber attack is a cost-effective, asymmetric, deniable tool that can be deployed with little risk of reprisal, as detection/ culpability is very difficult to establish. The attacks can be easily customised to use the internet and communication infrastructure of a third-party nation or organisation. The examples of cyber attacks quoted in the preceding paragraphs bring out the following:

- Disproportionately large scale damage can be caused by relatively small investments in the technology infrastructure and manpower resource.
- No explosive weaponry is required to disrupt the social, financial, political or technical equilibrium of nations.
- Cyber warriors can be more dangerous than the best equipped armed forces with conventional armaments.
- It is very difficult to prove culpability as the identity of the perpetrator can be easily concealed.
- The attacks are a convergence of easily available tools, technologies and expertise, access to which is not limited by geographical boundaries.
- Tools and techniques are interoperable between state and non-state actors.
- *Cyber warriors are not bound by the ethical rules of conventional war which binds uniformed soldiers of law abiding and responsible nations.*

In spite of the clear and present danger, it is surprising that nearly half the world's countries have neither drafted nor adopted a national cyber security policy or strategy till date to counter this threat. This not only leaves the parent nation's critical infrastructure and economy prone to cyber attacks, but also offers a safe haven for criminals to mount attacks on other nations or organisations. A study by the United Nations to map the commitment of nations towards cyber security was carried out by the United Nations' International Telecommunication Union (ITU) in the year 2017.[7]

From an Indian perspective, the survey only suggested that we have a fairly robust cyber ecosystem wherein laws, technical skills and organisational awareness are sufficiently developed to detect a cyber security breach. However, inter-agency partnerships and sectoral expertise, required to ensure a swift response, were found wanting.

CYBER SECURITY PREPAREDNESS QUOTIENT

The ITU's[8] sponsored survey measured the commitment of nations towards cyber security. The survey placed India[9] well above China in the Global Cybersecurity Index (GCI) 2017. Should this make Indians feel thrilled and content with the state of affairs in the cyber world? The answer to this question lies in the detailed analysis of the report and the parameters used for grading the countries. Some interesting facts are given below:

- The five key performance indicators used in the survey to rank the countries were: existence of legal apparatus, technical framework, organisational policy, Research and Development (R&D), investigation capacity and cooperation/ partnership model to enforce cyber security and foster economic development.

7. UN ITU 2017, *Global Cyber Security Index (GCI) Report 2017*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. Accessed on July 24, 2017
8. Ibid.
9. Reuters, "UN Survey Ranks India at Number 25 in Global Cyber-Security Index", *NDTV News*, July 5, 2017, http://gadgets.ndtv.com/internet/news/un-itu-global-cyber-security-index-survey-india-rank-1720990. Accessed on July 24, 2017.

It is a well-known fact that anti-virus and cyber security companies also have their own set of problems for not being able to quickly identify malwares. According to the NDTV Gadgets 360 magazine, only about two of the 60-odd anti-virus companies worldwide could detect the 'WannaCry' or 'Petya' malware in their first test iteration.

- It highlighted the gaps in the cyber security ecosystems of countries in terms of their awareness, understanding, knowledge/ capacity to deploy proper strategies and their capabilities/ programmes to counter cyber attacks.
- Countries were ranked in terms of their legal, technical, organisational skills, capacity building and cooperation on cyber awareness.
- Singapore topped the list as the country most committed to cyber security, the US came second, whereas Russia was ranked 11th, India 25th, China 34th and North Korea 57th.
- The survey only compared the preventive approach of nations. However, in the new world order, an offensive posture in cyber is also a popular method of defence and deterrence, and a force multiplier.

Therefore, from an Indian perspective, the survey only suggested that we have a fairly robust cyber ecosystem wherein laws, technical skills and organisational awareness are sufficiently developed to detect a cyber security breach. However, inter-agency partnerships and sectoral expertise, required to ensure a swift response, were found wanting. This means that India's sectoral threat detection mechanism is world-class but the response mechanism is not quick and coordinated to ensure minimal losses. This also means that the existing multi-dimensional organisational hierarchy at the apex level prevents cohesion of talent. The survey brought out many new facets of the cyber ecosystem.

Therefore, before analysing the gaps in the Indian cyber ecosystem and the methods to overcome them, it would be in order to discuss the various advancements in the technology of cyber threats. These developments have made detection difficult and defence increasingly convoluted.

CYBER THREATS: TECHNOLOGICAL ADVANCEMENTS

According to the Federation of Indian Chambers of Commerce and Industry's (FICCI's) Pinkerton India Risk Survey (IRS) 2017[10], which was released on June 23, 2017, information and cyber insecurity would be the biggest business risks in the near future. During the interaction following the release function, Mr Alok Joshi, chairman, NTRO (National Technical Research Organisation) pointed out that both industry and government need to have a collaborative outlook to address the emerging threat of information and cyber insecurity. He further advised that "despite these known risks, users just aren't good at keeping their *Windows OS* based services patched with security software updates".[11] It is a well-known fact that anti-virus and cyber security companies also have their own set of problems for not being able to quickly identify malwares. According to the NDTV Gadgets 360 magazine, only about two of the 60-odd anti-virus companies worldwide could detect the 'WannaCry' or 'Petya' malware in their first test iteration.[12]

Technically, most cyber security (anti-virus) algorithms (software) identify malware by their genetic coding pattern. For example, the ransomware virus usually attempts to lock user files available in hard drives, by encrypting them. Based on this characteristic of ransomware, most anti-virus programmes flag those encryptions as surreptitious that don't show an 'on-screen' progress bar. A similar logic is used by anti-virus software to identify malicious programmes by matching their code/ behaviour against a database of known malware. Therefore, the database of malware codes at each computer terminal has to be regularly updated by the software. This is ensured by the anti-virus company by frequently asking its users to download the latest patch. Purely from the perspective of cyber security, this technique is only as good as the database of malware, which is based on the fingerprints of known viruses. However,

10. Express News Service, "Cyber-Attack Top Threat to India Inc", *The New Indian Express*, June 24, 2017, http://www.newindianexpress.com/nation/2017/jun/24/cyber-attack-top-threat-to-india-inc-1620215.html. Accessed July 6, 2017.
11. Ibid.
12. Associated Press, "How Artificial Intelligence Is Taking on Ransomware", Gadgets 360, June 29, 2017, http://gadgets.ndtv.com/internet/features/ransomware-petya-wannacry-ai-based-defence-1718339. Accessed on July 28, 2017.

Another problem facing the cyber security environment is the unrestricted proliferation of cyber espionage tools and technology into the hands of non-state actors/ terrorist groups. Easy access to the internet has enabled these non-state actors to launch cyber attacks on behalf of their sponsors. These new groups are self-sustaining, technically qualified, highly trained and motivated.

simple reasoning would explain that a new variant of malware can easily slip through the database by changing its identity just before the next update gets installed.

To control this, anti-virus companies are now employing machine learning algorithms which identify and block malware, ransomware, botnets and Trojans[13]. SentinelOne[14] even offers a $1 million guarantee against ransomware. This demonstrates the growing confidence of anti-virus companies to new and better techniques. Clearly, this is a cat and mouse game between the hackers and anti-virus companies. Therefore, every ICT user needs to be aware of the cyber environment and make a determined effort to remain aware of the changing demography.

CYBER ESPIONAGE: ENABLER FOR DOMINANCE

War is a state of armed conflict between nations or different groups within a nation. While all wars involve espionage, not all espionage is war. A number of countries across the world are engaged in espionage or spying against each other for defensive as well as offensive reasons. Cyber espionage is a highly tactical tool which can be used effectively for information gathering as well as information denial. In some scenarios, it can also act as a very offensive weapon which has power

13. Trojan is a malware that disguises itself as legitimate software. It is employed by cyber-thieves and hackers to gain access to users' systems with an intention to spy and steal sensitive data. Trojans can delete, block, modify, copy data and/or disrupt the performance of computers or computer networks.
14. Sentinel One, "Protection Against Ransomware, Guarantee", https://go.sentinelone.com/rs/327-MNM-087/images/SentinelOne%20Ransomware%20Warranty%20v3.pdf, accessed on July 22, 2017.

to even topple governments[15] or threaten the sovereignty of nations. The methods of cyber espionage are continuously evolving. During its infancy, the approaches for cyber espionage were limited to defacement of government websites, denial of services, phishing of emails of government officials, spreading disinformation, etc. However, with time, the techniques of espionage have become more intelligent, advanced and sophisticated. New malwares can easily violate the privacy of classified data sources, suppress the functioning of electronic control systems, disrupt public services and proliferate misinformation within seconds. Trojans written specifically for espionage can remain undetected for a considerable period of time and thereafter be remotely activated (or programmed) to attack critical infrastructure on a pre-defined date and/ or time. High end technology to hack into computer networks and take over its functioning is easily available at minuscule cost.

According to some media reports, countries have started engaging private agencies and individuals to extract classified information/ data from social media sites, ISPs, mobile companies, etc. The US government's NSA's Prism programme was an example of how government agencies got involved in acquiring data from private entities.

Another problem facing the cyber security environment is the unrestricted proliferation of cyber espionage tools and technology into the hands of non-state actors/ terrorist groups. Easy access to the internet has enabled these non-state actors to launch cyber attacks on behalf of their sponsors. These new groups are self-sustaining, technically qualified, highly trained and motivated. They also specialise in exploiting the legal and technical frameworks of countries for their nefarious activities. These non-state actors are a greater threat, as it is difficult to identify them and/ or challenge their intentions. Some of these non-state groups also have the potential to cause large scale disruptions to the world order.

15. The Panama Papers contained over 11.5 million leaked documents on personal financial information of more than 214,488 offshore entities, including politicians and corporate heads, leading to the resignation of heads of states of Iceland, UK, Brazil, Pakistan, etc.

The alarming reality is that some nations have started using the services of these non-state actors to further their own nationalistic or political agendas. History is witness to the fact that sophisticated network surveillance tools like GhostNet[16], Red October[17] and The Mask[18] were developed at the behest of state governments by non-state actors to sabotage selected organisations or government networks. Another hacking tool called RCS (Remote Control System) was used by many governments,[19] including Azerbaijan, Colombia, Egypt, UAE, and Uzbekistan, to eavesdrop on the activities of other nations.

According to some media reports, countries have started engaging private agencies and individuals to extract classified information/ data from social media sites, Internet Service Providers (ISPs), mobile companies, etc. The US government's National Security Agency's (NSA's) Prism programme was an example of how government agencies got involved in acquiring data from private entities. Similarly, nations like Israel, North Korea and Iran have also revealed their capability to take on technologically, economically and geographically mightier nations using the power of cyber space. It is alleged that North Korea has a clandestine connection with a hacking group called Lazarus. It is also believed that in the year 2016, the $81 million cyber heist on the Bangladesh Central Bank and the 2014 attack on Sony's Hollywood studio were carried out by this group. The US government has since blamed North Korea for the Sony hack, and government prosecutors from Bangladesh are building a legal case against Pyongyang in the bank theft.

This exemplifies that technology is breaching the barrier between legitimate and illegitimate usage, as the tools and methodologies of cyber offence

16. John Markoff, "Vast Spy System Loots Computers in 103 Countries", *The New York Times*, March 28, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html. Accessed on July 25, 2017.
17. Dave Lee," 'Red October' Cyber-Attack Found by Russian Researchers", *BBC News*, January 14, 2014, http://www.bbc.com/news/technology-21013087. Accessed on July 25, 2017.
18. Kim Zetter, "Sophisticated Spy Tool 'The Mask' Rages Undetected for 7 Years", *Wired*, October 2, 2014, https://www.wired.com/2014/02/mask/. Accessed on July 25, 2017.
19. Bill Marczak,Guarnieri, Morgan, and JS Railton, "Mapping Hacking Team's "Untraceable" Spyware", *The Citizen Lab*, February 17, 2014, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/. Accessed on July 25, 2017.

are similar. Further, investigations into cyber attacks also highlight the connection among organised cyber criminals, terrorists and ransomware benefactors and dark currency (bitcoin) financiers. This nexus between state and non-state actors is a dangerous trend, for which the traditional deterrence tactics prove ineffective. Therefore, new strategies and plans to protect the national interest have evolved in which cyber space is gaining centre-stage.

North Korean hackers acquired confidential data, including the personal details of workers, design manuals of nuclear reactors, electricity flow charts, etc of two nuclear power plants located close to Seoul operated by Korean Hydro and Nuclear Power (KHNP). This information was then shared on social media and a scenario crafted around it as though the security of the nuclear power plant itself had been breached.

CYBER ASTUTENESS IN MILITARY DOMAIN

Offence is the best way of defence in cyber space. An offensive cyber strategy not only strengthens the ecosystem, but also compels the adversary to reconcile its interventionist plans due to the fear of the unknown. Cyber astuteness can be defined as the ability of an organisation to quickly judge a situation and influence information and opinion by skilful use of cyber technology for commercial gains. It is a way to deploy defensive capabilities for offensive use. A few countries have mastered this skill and use it as a powerful strategy against adversaries by creating a narrative that influences public opinion. They have developed astute ways to use the internet as a weapon and target the social media, government information systems, infrastructures and utilities with the aim to cripple these socially or politically[20].

Military experts believe that a large number of nations are in a state of virtual and undeclared war, either directly or through proxies, with each

20. Russian cyber intruders tried to delete or alter voter data during the US election, Frank Vyan Walton, "Russian Cyber Hacks Breached Voting Systems in 39 States", Dailykos, June 13, 2017, https://www.dailykos.com/stories/2017/6/13/1671421/-Russian-cyber-hacks-breached-voting-systems-in-39-states. Accessed on July 24, 2017.

A CNO disrupts the adversary's cyber space by denial, degradation or destruction of networked computers with an intention to affect the flow of information or data and degrade its decision-making ability. Most nations have camouflaged their cyber offensive formations by designating them as SIGINT, crypto analysis or military information units.

other in cyber space. They are using soft skills to obtain critical big data and/ or disrupt/ corrupt/ manipulate the same for commercial/ political/ military interests. This classified data is then exploited to gain access to critical infrastructures. For example, North Korean[21] hackers acquired confidential data, including, the personal details of workers, design manuals of nuclear reactors, electricity flow charts, etc of two nuclear power plants located close to Seoul operated by Korean Hydro and Nuclear Power (KHNP). This information was then shared on social media and a scenario crafted around it as though the security of the nuclear power plant itself had been breached. This created panic amongst the locals, and an embarrassing situation for the South Korean government and the international nuclear safety monitoring agencies.

Full spectrum information superiority and dominance is crucial to influencing operations associated with war or Military Operations Other Than War (MOOTW). The conventional view is that information is power, therefore, more and more information is necessary to take measured decisions, whether in war or otherwise. In such a scenario, cyber warfare is a cost-effective, asymmetric, deniable tool that can be employed with little very little risk of reprisal. Presently, most information and data are digitised and transmitted over large networks of ICT devices. Computer Network Operations (CNOs)[22] are actions taken by militaries

21. Justin McCurry, "South Korean Nuclear Operator Hacked amid Cyber Attack Fears", *The Guardian*, December 23, 2014, https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack. Accessed on July 24, 2017.
22. Computer Network Operations (CNOs): use of cyber techniques by military establishments to infiltrate into hostile individual computers or networks to extract intelligence, sensitive or confidential data.

or intelligence organisations to leverage the potentials of the digital networks to gain information superiority and also prevent the enemy from using its own capability. CNOs also deal with protection of own ICT networks against unsolicited attacks and detection. A CNO has two main objectives:

- Computer Network Attack (CNA): This deals with utilising computer networks to design and perpetrate network attacks against targets or enemy computers and networks. It includes using computer networks to sneak / exploit / infiltrate into enemy or target networks or computers for the sake of extracting confidential information.
- Computer Network Defence (CND): This is used to respond to network attacks, exploitation and intrusions by the enemy or malicious users.

According to the Western media, Israel's Unit 8200 is one of the most active, potentially lethal and cyber astute units in the world. Unit 8200 operates a massive spying network. It is one of the largest listening bases of the world, capable of monitoring phone calls, emails, and other communications throughout the Middle East, Europe, Asia, and Africa. It also tracks movement of aircraft and ships across the globe. It is believed to maintain covert listening posts in all Israeli Embassies abroad, and monitor feeds from undersea communication lines.

A CNO disrupts the adversary's cyber space by denial, degradation or destruction of networked computers with an intention to affect the flow of information or data and degrade its decision-making ability. Most nations have camouflaged their cyber offensive formations by designating them as SIGINT (Signals Intelligence), crypto analysis or military information units. Further, such formations are never openly acknowledged by nations but speculative journalism and research data proves otherwise. Nations put forth different reasons for venturing into this domain. The

US created the NSA[23] (National Security Agency) under the Department of Defence to "collect, process and disseminate intelligence information from foreign electronic signals for national and foreign intelligence and counter-intelligence purposes, and to support military operations". It also tasked the NSA to prevent foreign adversaries from gaining access to classified national security information. Similarly, other nations have also created dedicated military organisations to protect their cyber space, citing concerns about possible attacks on intellectual property. It is speculated that Russia, China, the UK, North Korea and Israel are amongst the top five nations that have been exploiting cyber technology for acquiring information/ data about allies and adversaries. This data is then used as a tool for negotiation and to forward their own economic, political and military plans. A list of some military formations/ units engaged in cyber offensive/ intelligence is given below:

Table 1

Country	**Name of Organisation**
USA	NSA
Russia	Federal Security Service (Federal'naya Sluzhba Bezopastnosti)
UK	MI6/Defence Cyber Operations Group
China	PLA Unit 61398
Israel	Unit 8200
N. Korea	Unit 810

The development and use of these military units which focus only on cyber warfare, is a cause for concern. However, in the succeeding paragraphs, we shall discuss only the strategies adopted by Israel and North Korea. As regards the top four countries, they are permanent members of the UN Security Council, with veto powers on all military affairs. They are also fairly large military and economic powers. Therefore, they blatantly and overtly engage in cyber astuteness by monitoring the

23. NSA/CSS, "Frequently Asked Questions", https://www.nsa.gov/about/faqs/. Accessed on July 26, 2017.

cyber activities of all countries and their citizens. They justify these acts as being oriented towards maintenance of world peace.

Kim Heung-kwang, a former computer science professor in North Korea who defected to South Korea in 2004, has said that most of Pyongyang's cyber attacks are planned by Unit 810 for raising money for its overseas intelligence wing, Reconnaissance General Bureau (RGB).

According to the Western media, Israel's Unit 8200 is one of the most active, potentially lethal and cyber astute units in the world. Unit 8200 operates a massive spying network. It is one of the largest listening bases of the world, capable of monitoring phone calls, emails, and other communications, throughout the Middle East, Europe, Asia, and Africa. It also tracks movement of aircraft and ships across the globe. It is believed to maintain covert listening posts in all Israeli Embassies abroad, and monitor feeds from undersea communication lines.

A majority of Israel's cyber spies of Unit 8200 are recruited under the *Magshimim programme*[24] which professes to nurture the talent of young students. School students as young as those in the 9th grade are enrolled for a three-year programme on computer coding and cyber security. During the course, they study programming languages and computing theory, implement cryptographic protocols, reverse-engineer malware, and design computer network architectures. This platform is aimed at incubating their talent and ideas for the cyber world and expanding the pool of soldiers to serve in the Israeli defence forces elite cyber unit. Students from this programme also join the high technology industries across the globe after completion of their compulsory military service.

24. Christa Case Rryant, "Israel Accelerates Cyber Security Know-how as Early as 10th Grade", *The Christian Science Monitor-CSMonitor.com*, June 9, 2013, http://in.bgu.ac.il/engn/ise/Documents/workIsrael-accelerates-cybersecurity-know-how-as-early-as-10th-grade.Printed%20version.pdf. Accessed on July 22, 2017.

Presently, the Prime Minister's Office (PMO) through the National Security Adviser (NSA) monitors the functioning of the National Technology Research Organisation (NTRO), National Information Board (NIB) and National Cyber Coordination Centre (NCCC). These three verticals form the umbrella set-up to coordinate intelligence gathering and sharing of issues/ advice amongst ministries and departments.

On the other end, North Korea's Unit 810[25] is fast developing its cyber capabilities under the patronage of China. It has been recently blamed by officials and internet security experts for online attacks on the financial networks of various countries in order to finance its own overseas operations.

Kim Heung-kwang[26], a former computer science professor in North Korea who defected to South Korea in 2004, has said that most of Pyongyang's cyber attacks are planned by Unit 810 for raising money for its overseas intelligence wing, the Reconnaissance General Bureau (RGB). James Lewis[27], a North Korea expert at the Washington-based Centre for Strategic and International Studies, also opines that Pyongyang uses hacking as a tool for espionage and political harassment of South Korean and US organisations. North Korea is also suspected of staging cyber attacks against the South Korean nuclear reactor in 2014, through Chinese or Malaysian IP addresses.

CONVERGENCE OF CYBER CAPABILITIES: NATIONAL RESPONSE

Post the year 2014, traditional adversaries of the Cold War era realigned to form new alliances. These engagements were based on economic and

25. Reuters, "North Korea's Unit 180, the Cyber Warfare Cell that Worries the West", *The Asian Age, Technology, e-paper*, May 21, 2017, http://www.asianage.com/technology/in-other-news/210517/north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west.html. Accessed on July 6, 2017.
26. Dave Lee and Nick Kwek, "North Korean Hackers 'Could Kill', Warns Key Defector", *BBC News*, May 29, 2015, http://www.bbc.com/news/technology-32925495. Accessed on July 24, 2017.
27. James Andrew Lewis, *Report: North Korea's Cyber Operations* (New York: December 30, 2015) available online at https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations. Accessed on July 25, 2017.

commercial considerations rather than geographical proximities. The realignments also led to doctrinal changes in the methods of aggression. Conventional techniques of physical engagement of militaries on the ground gave way to methods which are more precise and devastating. A comparison of the approaches of different nations towards building up cyber capabilities clearly indicates the importance that governments have assigned to this new dimension of war. Different methodologies are being adapted by nations to develop strong cyber capabilities and refine the doctrinal framework. Nevertheless, the directions of future wars are clearly inclined more towards exploitation of cyber space rather than the use of explosives alone. Given the strong IT soft-skills available within the country, it is time India converges its defensive and offensive cyber capabilities to achieve military dominance.

More than 700 websites of central ministries/ departments and state governments were hacked between the years 2013 and 2016 (199 in 2016, 164 in 2015, 155 in 2014 and 189 in 2013)[28]. This fact was revealed in a written reply to the Lok Sabha by Shri Hansraj Gangaram Ahir, minister of state in the Ministry of Home Affairs on February 7, 2017. The signature of these attacks suggested that most of them originated from servers or proxies stationed/ traced to Pakistan or China. It is also believed that Pakistani agents frequently use social engineering for espionage, opinion moulding and anti-national narratives, while the Chinese agents indulge at the more strategic levels and target military and economic centres.

Presently, the Prime Minister's Office (PMO) through the National Security Adviser (NSA) monitors the functioning of the National Technology Research Organisation (NTRO), National Information Board (NIB) and National Cyber Coordination Centre (NCCC). These three verticals form the umbrella set-up to coordinate intelligence gathering and sharing of issues/ advice amongst ministries and departments. As per details hosted on official websites of various ministries and departments of the Government of India, there are over 35 different agencies functioning under the Prime Minister's

28. MHA, GoI, Reply to Lok Sabha unstarred question no. 806 to be answered on February 7, 2017, http://mha1.nic.in/par2013/par2017-pdfs/ls-072217/806.pdf. Accessed on July 24, 2017.

Training is another important method to contain the devastation of a cyber attack. Sectorial training schools are required to be set-up across the country to give specialised training to operators and ground staff to handle all types of emergencies involving the functioning of their networked computer.

Office, Ministry of Defence, Ministry of Electronic and Information Technology, Ministry of Home Affairs, Ministry of External Affairs (PMO, MoD, Meity, MHA, MEA) and various other ministries dealing with issues related to surveillance of cyber space, collection/ analysis of cyber intelligence and cyber security law enforcement. There are also sectorial Computer Emergency Response Teams (CERTs) with each ministry which have domain specialisation.

Having a large number of apex level agencies for management, coordination and supervision of cyber security has some advantages but also its own problems. Issues of overlapping and conflicting powers, functions, duties and responsibilities add up to ambiguity rather than synergy. Time is one of the most damaging components of a cyber attack. A delayed response can magnify the enormity of the damage. Therefore, cyber security should be treated as a collaborative function, and responded to with military precision.

Drawing inference from global inputs and the changing frontiers of warfare, the Joint Doctrine of the Indian Defence Forces was revised and released on April 25, 2017. The new doctrine emphasised on the development of a strong cyber agency and evolution of potent cyber warfare capabilities by India. The wherewithal for setting up of the new agency as well as the need to strengthen the existing IT security infrastructure was also finalised during the Unified Commanders' Conference, 2017. The conference was attended by Defence Minister Arun Jaitley, NSA Ajit Doval, the three Service chiefs and other senior military commanders. Concurrently, the Ministry of Defence also agreed to set up a new agency to bolster security infrastructure[29]. Accordingly, a Special

29. PTI News service, "Def Minister to Set up New Agencies to Bolster Security Infra", *PTI News*, July 11, 2017, http://ptinews.com/news/8878480_Def-Minister-to-set-up-new-agencies-to-bolster-security-infra. Accessed on July 18, 2017.

Operations Division that includes the cyber and space agencies has been planned under the Headquarters Integrated Defence Staff (HQ IDS).

WAY FORWARD FOR CYBER DOMINANCE

It is also important to synchronise the military and cyber capabilities of the nation to maximise their effect, as in the case of Operation Orchid. It would be naive to assume that adversaries would not vector the cyber forces along with military force against us. Therefore, there is a need to develop an environment within the country to fight this threat as well as to develop offensive outreach. The writing on the wall is loud and clear. Cyber space benefits from asymmetry and future military campaigns would be planned in tandem with cyber operations. Therefore, technological superiority in the cyber infrastructure, with synchronised offensive capabilities, is required to position India as a cyber secure country, where economic developments are not threatened by cyber attacks.

It is important to continuously invest in technology, skill, training and knowledge. Further, given the anonymous characteristics of cyber space, an urgent reconciliation of capabilities, responsibilities and response mechanism of all the departments involved in security of cyber space is required.

India has a vast army of young software engineers. These budding professionals have positioned the country as the software development hub of the world. There is a need to initiate a programme like the Magshimim programme of Israel where young talent (school and college students) can be incubated and tasked to develop specific cyber skills. Also, the enrolment norms for the military services may also be tweaked to make way for professionals to be enrolled for cyber specific tasks.

Training is another important method to contain the devastation of a cyber attack. Sectoral training schools are required to be set-up across the country to give specialised training to operators and ground staff to handle all types of emergencies involving the functioning of their networked computers.

They also need to be trained to notice any malfunction or misbehaviour in the operator's console so that an alarm can be raised.

Hackathons are open competitions or events in which professional and amateur computer programmers, software developers, project managers and end users collaborate to develop new software technologies or find innovative solutions to real life problems. They also provide a platform to check the vulnerability and stability of the existing software's security architecture. The first of its kind Hackathon was conducted by the Government of India for 36 hours on April 1-2, 2017. More than 42,000 students and professionals participated across 26 locations in India to find solutions to 598 problems. The entire event gave a new dimension to how the present government is looking forward to use cyber space and how committed it is to ensure that the ecosystem remains conducive for growth. This is a positive approach and conduct of such events at regular intervals should be encouraged. It will go a long way in harnessing talent.

Lastly, there is always a requirement to demonstrate the offensive cyber skill of the nation. *Demonstration of capabilities is required to deter the adversary from enterprising a misadventure.* Like the military might of the nation is put on display during the Republic Day parades and in international military exercises, similarly, cyber offensive skills should be demonstrated publicly during occasions like Technology Day, etc.

CONCLUSION

Cyber threats, today, have become more offensive and involve silent intrusion into the adversary's electronic networks. It is evident from the recent developments in cyber space that future military campaigns/ operations would be greatly assisted by ICT devices. As cyber space has the potential to deliver measured destruction, its smart use could change the course of operations. Therefore, countries are investing heavily into talent and technology for augmenting the capabilities of cyber space.

Concurrently, cyber criminals and hackers have no international boundaries. Therefore, it would be naive to imagine immunity from cyber aggression due to geographical distances or technical outreach. It is time that

all organisations, whether government run or privately owned, understand the pitfalls of an "unsecured" networked working environment. It is important to continuously invest in technology, skill, training and knowledge. Further, given the anonymous characteristics of cyber space, an urgent reconciliation of capabilities, responsibilities and response mechanisms of all the departments involved in the security of cyber space is required. Referring back to the ITU survey, it is time for India to strive to be included amongst the top 10 nations in the Global Cyber Security Index to match its aggressive development agenda. The policies and framework to counter cyber offences should be refined, along with a clear underlying intention and capability to go on to the offensive, if required. Only then can we claim to be a nation with a robust cyber security ecosystem.

Therefore, technological superiority in cyber infrastructure with synchronised offensive capabilities is required to position India as a cyber secure country, where economic developments are not threatened by cyber attacks.