Section V
Cyber Warfare

Military Domain of Cyber Warfare

S Kulshrestha

It would require sustained action for an adversary to take down a network for a period of time which would be really debilitating, but it is possible and something that we need to guard against and be concerned about.

Christopher Painter, the first cyber coordinator for the US State Department

The extent of cyber reach from dedicated attacks on strategic assets to tactical military operations to criminal activities like ransom to inconveniencing mass populations can be gauged from the following incidents:

The well-known Stuxnet strike, required a tremendous amount of resources, brainpower, and planning time. It falls under the one time gambit with major nations already on guard against similar strikes on their critical strategic facilities.

In 2009, the Conficker worm infected civil and defence establishments of many nations, for example, the UK Department of Defence (DoD)

Rear Admiral Dr S Kulshrestha (Retd), is Senior Fellow at New Westminster College, Canada. The views expressed are personal.

reported large-scale infection of its major computer systems including ships, submarines, and establishments of the Royal Navy. The French naval computer network 'Intramar' was infected, the network had to be quarantined, and air operations suspended. The German Army also reported infection of over 100 of its computers. Conficker sought out flaws in Windows operating system (OS) software and propagated by forming a botnet. It became the largest known computer worm infection by afflicting millions of computers in over 190 countries.

A cyber attack in December 2015 against energy distribution companies in Ukraine led to massive power outages and affected a huge civilian population. This achieved high visibility while using an old Trojan, BlackEnergy and other malware to shut down critical systems and wiping out data.

The Hollywood Presbyterian Medical Centre in Los Angeles, California, was the victim of a cyber attack in February 2016 that encrypted its electronic data, rendering its systems unusable for over a week. The hospital was forced to operate with no access to its computer systems and even had to move some patients to other hospitals. The hospital regained access to its data only after paying a fee of 40 bitcoin (approximately US$ 17,000) to the attackers. Since 2014, the CryptoLocker ransom ware alone has allowed cyber criminals to collect over US$ 100 million. The San Francisco Municipal Transportation Agency (SFMTA) was hit with a ransom ware attack on 25 November 2016, causing fare station terminals to carry the message, 'You are Hacked. All Data Encrypted.[1] The hacker sought a ransom of Bitcoin 100 (~US$ 76,000). Interestingly, the hacker behind this extortion attempt had been hacked himself, revealing details about other victims as well as clues about his identity and location.

According to a Forbes news report in November 2016, anyone could rent an army of 100,000 bots for US$ 7,500 on the dark net. Its controllers boasted that the Mirai-based botnet could unleash attacks of one terabit per second or more.[2] Mirai malware enables computer systems running on Linux into remotely controlled 'bots' that can be used as part of a botnet in large-scale network attacks. It targets online consumer devices such as remote cameras and home routers. The Mirai botnet has been used in some of the largest and most disruptive Distributed Denial of Service (DDoS) attacks since October 2016.

While illustrating the wide ambit under which cyber attacks take place and the enormous cyberspace that is vulnerable, the earlier mentioned examples also highlight the inevitable ease of the threat to the military and civilian space.

Cyberspace is time-dependent set of interconnected information systems and human users that interact with these systems.

The North Atlantic Treaty Organisation's (NATO's) Cooperative Cyber Defence Centre of Excellence (CCD CoE) defines cyberspace as, 'Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.'[3] The tsunami of networked devices is expanding the cyberspace exponentially along with the requirement of data by individuals, corporations, militaries, and governments. Cyberspace is becoming increasingly vulnerable to hostile and unscrupulous interjections; unfortunately, the cyber security aspects are lagging far behind the complexities of the emerging cyberspace. Various factors of cyberspace favour the attackers—importantly among them are its nebulous nature and its dynamic, which leads to ease of switching and concealing identities. These imply that it is extremely difficult to impose punitive measures against them and that such attacks would continue despite the advances in firewalls and other cyber protection systems.[4]The cyber attackers make use of vulnerabilities like inadequacies in software, use of secretly tampered hardware, interfaces between software and hardware like reprogrammable RAMs, online connectivity, use of user enabled settings, and access to malintentioned personnel who can infect directly or enable remote access. The attacker could target specific computers or carry out a general attack by delivering a payload that can activate at a given time.

To achieve clarity in the military domain of cyberspace, a few more definitions are necessary. Computer Network Operations (CNOs) is a broad term that has both military and civilian applications. It is considered one of five core capabilities under Information Operations (IO) of Information Warfare (IW) by the US military. In the *Dictionary of Military and Associated Terms,*[5] cyber operations are defined as, 'the employment of cyber space capabilities where the primary purpose is to achieve military objectives or effects in or through cyber space.'[5] According to the US Joint Doctrine for Information Operations,[6] CNOs consist of Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).[6] Computer Network Attack (CNA) includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves. Computer Network Defence (CND) includes actions taken via computer networks to protect, monitor, analyse, detect and respond to network attacks, intrusions, disruptions or other unauthorised actions that would compromise or cripple defence information systems and networks. CNE includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks. CNOs, in concert with Electronic Warfare (EW), are used primarily to disrupt, disable, degrade, or deceive an enemy's command and control, thereby crippling the enemy's ability to make effective and timely decisions, while simultaneously protecting and preserving friendly command and control.

Offensive cyber operations, from a military point of view, can be referred to as 'actions taken in the cyber environment to deny the actual or potential adversary's use of, or access to, information or information systems, and affect their decision-making process.[7] Offensive cyber operations cover the full spectrum of cyber war, commencing with covert special operations to regular to overt strategic cyber operations. Deploying of offensive cyber capabilities against the attacker would be difficult for a nation state in view of the lack of evidence and/or identity of the aggressor.

According to the US DoD, Offensive Cyberspace Operations (OCO) are 'intended to project power by the application of force in and through cyberspace. OCO will be authorized, like offensive operations in the physical domains, via an Execute Order (EXORD).'[8] These offensive cyber operations however, are to be used discriminatingly. 'Military attacks will be directed only at military targets. Only a military target is a lawful object of direct attack.' However, military targets are defined broadly as 'those objects whose total or partial destruction, capture, or neutralization offers a direct and concrete military advantage.'[9]

The strategic cyber attack presents a powerful option of crippling a conventionally superior nation by being obscure and averting a conventional military strike.

Richard Clarke, the former US National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, in *Cyber War: The Next Threat to National Security and What to Do About It,* defines cyber war as, 'actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.'[10] There could be various objectives of a cyber attack on military facilities; these could range from causing damage to the software of the system and/or the network, they could lie hidden and inject spurious messages, deny or degrade service, disable encryption systems, alter resident data, etc. Cyber attacks have also been divided into two categories by some experts as syntactic attacks that act directly, and semantic attacks that aim to modify data. The syntactic attacks are directed onto Information Technology (IT) facilities, and semantic attacks target users.

A plausible strategic cyber attack scenario is as follows:

> As India races towards digitisation in its infrastructure and related networks, a strategic cyber attack by Pakistan (proxy China) on India, a few years hence could unfold by targeting critical infrastructure in the civil and military domains. It could commence with large scale casualties (possibly in thousands) across India, resulting from disruptions, chaos, and accidents in railways and civil air traffic; it could collapse communications; cripple the road/metro traffic in cities; graduate to failures in essential services like the electric, water supply and hospital services; depending upon the level of interconnectivity, lead to a collapse of the goods supply chain and uncontrollable fires.

This scenario, to a large extent, is a distinct possibility even today.

Some salient features of strategic cyber attacks are relevant. The strategic cyber attack presents a powerful option of crippling a conventionally superior nation because of its far cheaper costs, its remaining obscure, thus, averting a conventional military strike, its ability to inflict hard damage and result in long-term loss of men and material, its being technologically superior, with near a instant launch capability at very large distances, and, lastly, the fact that it is beyond the realm of any international legal framework.

However, it is also true that putting cyber weapons in the same league as nuclear weapons would not be correct because cyber weapons cannot replicate the damage potential of nuclear weapons nor do they have the ability to assure destruction to the levels that grant them a status of deterrents. As of now, strategic cyber weapons have never been used and have not contributed to victory in a military war. They have yet to shift the balance of power on the battlefield and accredit themselves with a certified victory.

China Factor

China has undertaken modernisation of its cyber capabilities under what it calls informationisation. It is an effort by the People's Liberation Army (PLA) to attain a fully networked force status. The aim of this process is to maintain information superiority and dominance against the adversary. China is developing a comprehensive computer network exploitation capability to gain strategic intelligence about likely aggressors and their allies as a precursor to winning future conflicts. The overall aim is to synergise computer network operations, electronic warfare, and kinetic strikes to cripple the enemy's information infrastructure. It has adopted Integrated Network Electronic Warfare (INEW) that consolidates the offensive mission for both Computer Network Attack (CNA) and EW under the PLA General Staff Department's (GSD's) 4th Department (Electronic Counter-Measures).[11] The Computer Network Defence (CND) and intelligence gathering responsibilities are assigned to the GSD 3rd Department (Signals Intelligence), and a variety of the PLA's specialised IW militia units. The PLA is choosing its personnel from the Chinese civilian sector to induct a qualified workforce with specialised skills from commercial industry and academia. There are circumstantial links between China's exploitation and theft of key intellectual property from technology-based industries via cyberspace and the PRC's economic development goals. Dmitri Alperovitch of McAfee had compiled a report, *Operation Shady RAT* in 2011, that highlighted the hacking of more than 71 corporations and government entities around the world by a single entity using the Remote Access Tool (RAT), from 2006 to 2011.[12] Mandiant's 2013 report *APT1: Exposing One of China's Cyber Espionage Units,* claims that the PLA's cyber unit 61398 is most likely behind such exploitation on behalf of the PRC's military and economic goals.[13]

Taking cognisance of enhanced Chinese cyber warfare capabilities, the US Department of Defence Strategy for Operating in Cyber Space, 2011, had outlined five strategic initiatives. These are as follows:

- Treat cyberspace as an operational domain to organise, train, and equip so that the DoD can take full advantage of cyberspace's potential.
- Employ new defence operating concepts to protect the DoD networks and systems.
- Partner with other United States government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
- Build robust relationships with the United States allies and international partners to strengthen collective cyber security.
- Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

The US DoD in its cyber strategy for 2015 has set five strategic goals for its cyberspace missions.[14] These are as follows:

- Build and maintain ready forces and capabilities to conduct cyberspace operations.
- Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
- Be prepared to defend the United States homeland and its vital interests from disruptive or destructive cyber attacks of significant consequence.
- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Conclusion

In June 2016, a likely cyber attack on the Indian government and commercial organisations by Chinese military's Western Headquarters was carried out.[15] An alert was issued to the Indian armed forces that a Chinese Advanced Persistent Threat (APT) group called Suckfly, based in Chengdu region, is targeting Indian organisations, with the defence establishments as its prime targets. Suckfly is involved in conducting cyber espionage activities by sending a malware called Nidiran.

One thing that is certain is that cyber attacks in all forms and variations are going to increase exponentially in the military as well as civil arenas. This interim period of development of strategic cyber weapons accords an opportunity to a nation like India to put in place its cyber offence and defence policies and enhance its cyber capabilities to meet all eventualities in the future.

India has started thinking of setting up its own cyber-military industrial complex, and a proposal for automated cyber-defence was submitted in early 2016 for platform to be developed jointly by public and private bodies.[16] The proposal is supposedly based on the US DoD Cyber Strategy. It caters to the sharing of cyber attack indicators across the cyberspace domain in India.

The future cyber warrior in the military domain may not confirm to the rugged and tough image of the soldier of today. He/she may be a person with mediocre health but with a cyber aptitude and capability that could collectively outshine India's enemies.

Notes

1. San Francisco Rail System Hacker Hacked, 29 November 2016 available at https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/, accessed on 05 December 2016
2. Mathews Lee, World's Biggest Mirai Botnet Is Being Rented Out For DDoS Attacks, 29 November 2016, available at http://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#6040253c3046, accessed on 05 December 2016
3. R Ottis and P Lorents, *Cyberspace: Definition and Implications,* Tallinn: Cooperative Cyber Defence Centre of Excellence, CCD CoE, 2010, available at https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html, accessed on 06 December 2016
4. IRI Porche, JM Sollinger, and S McKay, *A Cyberworm That Knows no Boundaries,*

Santa Monica: RAND National Defense Research Institute, 2011, available at http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf, accessed on 03 December 2016

5. *JP 1-02 Dictionary of Military and Associated Terms,* Washington: US DoD, available at https://fas.org/irp/doddir/dod/jp1_02.pdf, accessed on 05 December 20166. *JP 3-13 Joint Doctrine for Information Operations,* Washington: US DoD, available at https://fas.org/irp/doddir/dod/jp3_13.pdf, accessed on 07 December 2016
7. M Bernier and J Treurniet, *Understanding Cyber Operations in a Canadian Strategic Context: More Than C4ISR, More Than CNO,* Tallinn: CCD COE Conference on Cyber Conflict Proceedings 2010, available at https://ccdcoe.org/publications/2010proceedings/Benier%20-%20Understanding%20Cyber%20Operations%20in%20a%20Canadian%20Strategic%20Context%20More%20than%20C4ISR,%20More%20than%20CNO.pdf, accessed on 05 December 2016
8. Aftergood Stevan, Offensive Cyber Operations in US Military Doctrine, 22 October 2014 available at https://fas.org/blogs/secrecy/2014/10/offensive-cyber/, accessed on 03 December 2016
9. Cyberspace Operations, JP 3-12 (R), available at http://fas.org/irp/doddir/dod/jp3_12r.pdf, accessed on 03 December 2016
10. RA Clarke and R Knake, *Cyber War: The Next Threat to National Security and What to do About It*, New York: Ecco, 2010.
11. US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, 2009, available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf, accessed on 08 December 2016
12. Dmitri Alperovitch, Revealed: Operation Shady RAT, available at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, accessed on 08 December 2016
13. Exposing one of China's cyber espionage units, 23 February 2013 available at https://chinadailymail.com/2013/02/23/mandiant-executive-summary-exposing-one-of-chinas-cyber-espionage-units/, accessed on 08 December 2016
14. US Department of Defence Cyber Strategy, 17 April 2015, available at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed on 08 december 2016
15. Defence Forces on Alert After Chinese Cyber Attack, 12 June 2016 available at http://www.indiandefensenews.in/2016/06/defence-forces-on-alert-after-chinese.html, accessed on 07 December 2017
16. Singh Pukhraj, Cyber: The War India Never Fought, But Lost, 14 January 2016 available at http://www.huffingtonpost.in/pukhraj-singh/cyber-the-war-india-never-fought-but-lost/, accessed on 07 December 2017