“Based on advice provided to me by our cyber experts, Australian organisations are currently targeted by sophisticated state-based cyber actor”, Australian Prime Minister Scott Morrison informed Parliament last week. Prof. Alana Maurushat, an expert in Cybersecurity at Western Sydney University, cast all the blame on China owing to a current political and diplomatic tussle between two countries. In this regard, let’s dwell upon the cyber capability of two superpowers i.e. U.S. and China.

An unprecedented technological disruption, barging into each and every aspect of life, be it social, political, economic or strategic, has been at the helm of all affairs invariably. Unlike conventional warfare, cyber warfare is a constant war with personnel out on the battlefield round the clock. Even a slightest of mishap can compromise the entire security structure. Realising the importance of this new era warfare, wherein, for instance, operations as big as a nuclear exercise can be done through a simulated nuclear explosion, both China and USA have taken a stride in cyberspace security by inducting PLA UNIT 61398 (arguably) and US Cyber Command (USCYBERCOM) respectively.

Evolution

Cyberspace, as defined by US National Military Strategy for Cyber Operations, is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via the networked system and associated physical infrastructure. This digitized notional environment is the warehouse of extremely critical and sensitive information relating to government nuclear functioning, country's overall governance system, Cyberinfrastructure related to command and control system etc. Keeping this vulnerability in mind, USA commissioned United States Cyber Command (USCYBERCOM) in 2009 (operationalized in 2010). It was believed then, and rightly so, that cyberspace is going to be a new theatre of great power competition as other US military commands are extremely dependent and has enhanced stakes in its survivability. According to a report, the US Defence Department's Information Network is targeted by nearly 40 million malicious e-mails every day. Recently, the US celebrated 10 years of CYBERCOM. Gen. Paul N. Nakasone, commander of USCYBERCOM exclaimed "the world looked very different in 2010. We had no cyber mission force, our adversaries were different in numbers and sophistication and the Department of Defence was wrestling how cyberspace demands. Now we have a well-trained force, we have capabilities and most importantly we have delivered success." The strength of US Cyber network prowess can be effectively gauged by a statement from Ex-CIA Spy turned whistleblower, Edward Snowden's book 'Permanent Record' where he says "I sat at a terminal from which I had practically unlimited access to the communication of nearly every men, women and child on the earth who had ever dialled a phone or touched a computer."

There has been a greater sensitivity, particularly with the Chinese Communist Party (CCP), to manage and regulate cyberspace in a manner to protect it from outside infiltration and domestic enlightenment. As per a report released in 2013 by Mandiant, a US Cyber Security company, PLA Unit 61398 is a Military Unit Cover Designator (MUCD) of PLA responsible for the majority of cyber espionage campaign against foreign governments and the private companies. In 2014 Cyberspace Administration of China (CAC) was established as a central agency for internet regulation, Censorship, oversight and control of cyberspace. China, with the institutional support of Ministry of State Security (MSS) and to bridge the gap between its cyber capabilities and those of US, established PLA Strategic Support Force (PLASSF) in 2015 marking the beginning of Chinese Military Cyber Power and informational Operations capability. In the same year, National Defence White Paper titled 'China's Military Strategy' called for PLA to expedite development of cyber force, enhance cyber 'situation awareness capability' and cyber defence. Chinese Cyber power also provides Ideological dimension to

'state security'. Strict regulation over internet ensures domestic legitimacy to the authoritatively controlled regime and provides fodder to the propaganda apparatus of CCP to launch an informational war. To quote an abstract from IISS's Asia Pacific Regional Security Assessment 2019, "For PLA psychological warfare is an integral element of information operations in conjunction with cyber and electronic warfare." In recent times China has been involved in diplomatic (against Australia) and military (in the South China Sea and at LAC) standoff in its periphery. This assertive posturing has been followed by a massive mobilisation of the cyber army.

Image source: CNN

Contestation between Chinese and US Cyber Army

With the advent of cyberspace, there came an inexorable interlink between intelligence services and cyber armies around the world. The combination of these two have explored, at length, the resilience of governments to the modern technological disruption. Some of the cyber operations that left a significant imprint in the domain of cyber warfare are discussed

here.

China has been accused by the west for cyber governmental espionage, cyber commercial espionage, Intellectual Property theft etc. for years. Recently the US has accused China of spying the critical cyberspace through Huawei telecommunications equipment company by getting access to 'technological backdoor' build for law enforcement agency. Mallory episode of 2017 was another Chinese espionage offensive. Kevin Mallory, a CIA and Defence Intelligence Agency Officer, was under financial vulnerabilities when he was lured by fake Chinese think tank recruiter. Having conspired to share government's several top-secret documents and still-classified spying operation, he ended up in prison sentenced under the Espionage Act for 20 years. China has also been accused of Intellectual Property and technological theft which helped them develop clone applications such as Wechat, Weibo etc.

Not to forget, the biggest USA's intelligence and espionage scandal broke out in 2013 when Edward Snowden, an Ex-CIA systems analyst, leaked a significant amount of secret documents detailing secret spying operations, classified documents relating to surveillance and monitoring operations. He revealed that among 61000 hacking operations, network backbones like huge internet routers of Chinese Universities, public officials and businesses were hacked. Recently President Trump has asked US Intelligence agency to probe the origin of Coronavirus and possible nexus between WHO and China. In the United States, ethnic Chinese Americans are the prime target of US intelligence on a regular basis in their course of life. In a bid to claim the position of superpower both the countries have been reducing the individual rights with impunity.

Conclusion

What we, as a scholar or reader need to understand is that cyber warfare does not necessarily require a political environment to be operational. It's very much a part of regular power politics that puts a nation at an advantageous position over others in order to gain a strategic edge at times of strains. When the stakes are so high, as the question of superpower competition between USA and China, a slight moment of complacency can push a player out of the game. At the height of suspicion and at the brinks of the cold war between USA and Soviets, George Koval, a Soviet Spy, got access to the site of US Manhattan Project as an army sergeant, health inspector for radiation. Fast forward to 2007 he was posthumously awarded a 'Hero of Russia' medal for infiltrating secretly in US Manhattan Project and help the Soviet Union significantly to speed up manufacturing of nuclear bomb. Today, with so much technological advancement and cloud storage system,

such infiltrations can practically be done sitting in an office at any corner of the globe. So the cyber world needs constant vigilance and two decades down the line in 21st Century, US and Chinese Cyber Army are battling hard to restrict any strategic cyber advantage to the other.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments