WHY CHINA WILL PURSUE CYBER WARFARE MORE AGGRESSIVELY?

Wg Cdr MK Sharma

Research Fellow, CAPS

The New York Times (06 May 2013) carried a story claiming that People's Liberation Army (PLA) Unit 61398 near Shanghai has been identified as the likely source of many of the biggest thefts of data from Asian and American companies and government institutions.[1] On the other hand, in the last couple years, China's leaders have invested heavily in advanced short and medium range conventional ballistic missiles, land attack, anti ship cruise missiles, counter space weapons and military cyberspace weapons to substantially enhance its Anti Access /Area Denial (A2/AD) capabilities. The commissioning of China's first aircraft carrier *Liaoning,* development of Advanced Fighter Aircraft and limited regional power projection are but steps in the same direction. However, these fall well short of the military might (vis-à-vis US) required for a more assertive Chinese role on the world stage. In the transition period therefore, China is relying on its established pattern of warfare pivoted around asymmetry and technology transfer. Towards this China has developed several asymmetric and highly devastating weapons, such as a limited but modernising Nuclear Weapons capacity, China's Anti Satellite (ASAT) capability, and its electromagnetic pulse (EMP) capability. However, it remains interesting to see why Cyber Warfare capability tops this list of asymmetric weapons for China for the near future.

Why China will not use ASAT?

It is unlikely that China would use kinetic kill weaponry, such as its direct ascent Anti Satellite (ASAT), in an attempt to disrupt US space based assets. To disrupt US satellite dominance would require a massive sky clearing operation, because the US has constellations of satellites with

[1]http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=0

☞BACK TO WEBSITE

multiple redundancy. The US Global Positioning System (GPS) provides tactical communication and precision navigation, making it a desirable target however, the GPS uses at least five space satellite constellations. When one is destroyed, others can be manoeuvred to fill holes in the net. Not all of these satellites are within striking range at any given time. This means a sky clearing operation would take a significant amount of time, thereby revealing Beijing's intentions. This would cause international dispute due to space debris, and allow the US to manoeuvre its other satellites out of ASAT's way. It would also risk retaliation in which China would be at a disadvantage.

Additionally, there is no guarantee that such an attempt would be successful, as each launch requires precise targeting, and China's ASAT has only been tested once. It is more likely that China would attempt to knock out the corresponding relay stations on Earth by using a cyber attack. Chinese tacticians have focused on neutralising the uplinks and downlinks of the space-based systems through diverse forms of cyber attack including basic Distributed Denial of Services (DDoS) attack. This gives the advantages of deniability and low cost. It would remove distance from the equation, allowing multiple targets to be engaged simultaneously regardless of location, and it would dilute if not eliminate international condemnation and/or involvement.

Why China will not use Nuke?

China could destroy a vast majority of US electronics, including computers, cars, phones, and the power grid, using EMP weaponry. This is something of which all nuclear armed states are capable by means of high altitude nuclear explosions, taking as few as three nuclear bombs to blanket the continental US. It is now public that the US, China, France, and Russia all are using an EMP burst as a surprise first strike in war games as reported upon by numerous sources.[2] However, it is unlikely China would use such brute-force tactics. Using a high altitude atomic burst would cause

---

[2] Hearing on "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities" Tuesday, 20, May, 2008 Room 562, Dirksen Senate Office Building First Street and Constitution Avenue, NE Washington, DC 20510.
http://www.uscc.gov/hearings/2008hearings/agenda/08_05_20agenda.pdf

Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare*. (PLA Literature and Arts Publishing House, Beijing), February, 1999. http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf

Bartlett, Roscoe. "Nuclear Electromagnetic Pulse", *US Congressional Record*, 9 June, 2005. http://cryptome.org/bartlett-060905.txt
www.icnnd.org/research/New_Weapons_Technology.pdf

☞ BACK TO WEBSITE

international outrage as it violates an international treaty, it damages the environment, and it indiscriminately disrupts everything in its blast radius. Alternatively, shutting down the US power grid, production lines, water utilities, chemical plants, telecommunications, and transportation routes are possible through cyber attack, and it would provide the benefit of deniability also.

Cyber Warfare for Buying Time

Chinese military doctrine and strategy remain focused on modernisation. Beijing has not explicitly laid out an official grand strategy. This may be due to disagreement within the government, or done intentionally to hide the true motives and avoid being bound by them. However, several points which are evident include modernisation of weapons, equipment and training; accelerating the RMA; improving education and training of the PLA and the CPC (The Communist Party of *China*); "informationised" (*xinxihua*) warfare; and scientific development. China seeks to maintain domestic and regional stability while developing its economic, military, technologic, scientific, and soft power. It also seeks a balance between military and economic development, believing they are mutually dependent. At this juncture, while China tries to match its military power with US, it is buying time by keeping a low profile and depending on cyber reconnaissance. Cataloguing adversary weaknesses not only provides an asymmetric advantage in the event of a conflict, it also acts as a deterrent while China catches up in traditional military might. By utilising cyber reconnaissance, China can also accelerate its advancement in hi-tech weaponry.

Cyber Warfare for Technology Leapfrog

Espionage and technology transfer prosper in cyber warfare, where being physically present is not required, and attribution becomes increasingly difficult. It also falls in line with China's strategy of leapfrogging. By acquiring foreign military knowledge, China can quickly catch up and begin working at a comparable level, rather than investing the large amounts of time and effort it would take to acquire this knowledge independently. Interestingly, China's use of espionage to obtain foreign military technology is not restricted to any particular country. In 2007, the head of a Russian rocket and space technology company was sentenced to 11 years for passing sensitive information to China.[3]

[3] http://www.international-relations.com/CM8-1/Cyberwar.pdf

☞ BACK TO WEBSITE

Why Beijing would pursue cyber warfare is based on the basic premise that cyber warfare is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance. By using cyber warfare, China could achieve the same asymmetric destructive power while bypassing the drawbacks. China currently lacks the power projection to protect critical sea lanes from disruption or to deter international criticism. Crucial to the extended power projection is the blue water navy which would benefit from an online technology transfer and the further development of C4ISR. Online PSYOPS and media warfare would enhance China's soft power. Till such time Beijing builds up its military might and economy for its envisaged assertive global role, Cyber Warfare remains the best form of asymmetric warfare available.

☞ BACK TO WEBSITE