RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 032 – 11 February 2016



# The Real Star Wars: Improving Satellite Defences

*By Michael Raska*

## Synopsis

*Space is becoming increasingly vital to national security with space systems - satellites and spacecraft in orbit, ground stations, and communication systems - vulnerable to a range of cyber threats that may neutralise these assets.*

## Commentary

THE UNITED States, Russia, and China are currently spending billions for improving their satellite defences - primarily by building more capacity into their constellations and improving tracking abilities. In 2014, for example, Lockheed Martin was awarded a US$900 million contract to develop a radar system capable of tracking objects as small as baseballs in space in real time. Going forward, these and other countries will likely explore new ways to equip their satellites with active defences and countermeasures, such as jamming devices and the ability to evade both cyber and kinetic satellite interceptions.

The accelerating globalisation of space activities has intensified international competition and cooperation in the development of space-based capabilities. The 2011 unclassified version of the US National Security Space Strategy - the first national security space strategy co-signed by the secretary of defence and the director of national intelligence - points to three key trends shaping the current and emerging space environment: “space is becoming increasingly congested, contested, and competitive”.

## Cyber Threats to Satellites

According to the Union of Concerned Scientists, there are at least 1,300 satellites

now orbiting the Earth, with diverse military, civilian and commercial applications. The majority - 549 - are American while Russia has 131, China has 142, and India controls 33 satellites in orbit. Over 60 countries are investing in long-term space programmes.

In the civilian and commercial domains, nearly every cutting-edge technology adopted has strategic and operational dependencies on undefended satellites. For example, based on UK's intelligence assessments cited in recent press reports, 67 percent of the country's economy is dependent in some way on space-based communications. Another report produced for the US Department of Homeland Security in 2015 estimates that at least $1.6trillion of business revenues in the U.S. were "heavily influenced" by satellites.

In 2014, a number of think-tanks, including the Council on Foreign Relations and the Chatham House, warned of diverse cyber threats to space systems. These may include using backdoors in software that would enable an undetected remote access, the prevalence of unsecured software, non-protected protocols, and the use of unencrypted channels. One of their key recommendations was to immediately remove software updates from the public websites of select companies that provide satellite services and equipment, in order to prevent hackers from reverse-engineering the source codes.

Inherently, a loss of satellite communications would have cascading effects on the entire critical information infrastructure – from logistics land, air, and maritime traffic navigation, banking systems, media, to mobile global communications.

**Military Applications**

In the military domain, virtually every operational mission by advanced militaries relies on select space capabilities to enhance the effectiveness of the force. In the US military, the conceptual foundation is the Joint Publication (JP) 3-14, *Space Operations*, which details the strategic integration of military activities in the space domain with those in the traditional domains of land, sea, and air.

The latest version of JP 3-14 (May 2013) addresses the fundamentals of military space operations, the command and control of space forces, the roles and responsibilities of Service components, and the methods of planning for space operations. Specifically, JP 3-14 identifies five major mission areas: space situational awareness; space force enhancement; space support; space control; and space force application.

China is also substantially investing in advancing its civil and military space platforms and capabilities supported by extensive organizational infrastructure, research and development facilities, and increasingly more capable defense industrial base.

It is not yet clear whether the PLA has promulgated a formal doctrine solely for military space operations. Rather, PLA writings emphasise a holistic perspective toward space, cyberspace, and the electromagnetic spectrum that must be defended to achieve information dominance (*zhi xinxi quan*) - the ability to gather, transmit, manage, analyse, and exploit information, and preventing an opponent from doing

the same as a key prerequisite for allowing the PLA to seize air and naval superiority.

To this end, the PLA recognises the importance of controlling space-based information assets as a means of achieving true information dominance, calling it the "new strategic high ground". Consequently, establishing "*zhi tian quan*" (space dominance) is an essential component of achieving "information dominance".

According to studies by Kevin Pollpeter, China's space programmes serve two critical missions for the PLA: (1) Force Enhancement to support combat operations and improve the effectiveness of military forces such as ISR, integrated tactical warning and attack assessment, command, control, and communications; navigation and positioning, and environmental monitoring. (2) Counter-Space Missions to protect PLA forces while denying space capabilities to the adversary. To meet the demands, the PLA envisions three main capability requirements for space operations: the ability to enter space, to exploit space, and to control space.

**Strategic Implications**

The strategic significance of space will likely increase as satellite networks provide backdoors into almost every nationally important computer network or infrastructure – civil, commercial, and military. Notwithstanding traditional ballistic missile anti-satellite kills (ASAT), launching a cyber attack on satellites has three key advantages:

Firstly, attacks do not have to result in an uncontrollable debris cloud in outer space. Secondly, cyber attacks on satellites are also far cheaper for would-be assailants and, if done well, it can be almost anonymous. Thirdly, and perhaps most importantly, cyber attacks on satellites that disrupt or gather intelligence on other countries' infrastructure without the ability to respond, mitigate the prospects of early warning and deterrence.

*Michael Raska is Assistant Professor at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.*