Testimony before the U.S.-China Economic and Security Review Commission

Hearing on "China's Advanced Weapons"
Panel on China's Directed Energy and Electromagnetic Weapons Programs

Mr. David D. Chen, Independent Analyst[i]

23 February 2017

To Chairman Bartholemew, Senator Talent, and the Commissioners of the USCC, I offer my sincere thanks for being invited to speak today about such an interesting and emerging topic of analysis. I am also grateful to be sharing the floor with such an esteemed panel of experts. I also want to thank Commissioner Wortzel for forwarding my name.

BLUF: China has the engineering and spaceflight expertise, the doctrinal underpinnings, and the computer science and electrical engineering research and development experience for a counterspace cyber-EW directed energy weapons R&D program. My analysis stems entirely from open sources, based on academic research papers, journals, and other content published within China and internationally.

China's Growing Expertise in RPO Technologies

In the last ten years, China has launched half-a-dozen space missions, to date, with a suite of technologies for conducting what is known as "rendezvous and proximity operations" (RPO) (See Table 1). These include satellites which have been used to maneuver with and observe target spacecraft, such as Banfei Xiaoweixing-1 and -2, the first of which was launched by the Shenzhou-7 manned mission and infamously passed within 50 km of the International Space Station.[1] These also include the Aolong-1, launched in June 2016, a satellite equipped with a robotic manipulator purportedly for de-orbiting space debris, but which even an expert at the Chinese Academy of Sciences says is an "unrealistic" mission.[2] And in November 2016, the Shijian-17 satellite was launched, with a suspected inspection or signals intelligence mission, bringing Chinese RPO technologies into the geosynchronous belt for the first time.[3]

Why is this relevant for our discussion today on directed energy and other advanced weapons? Quite simply, due to the inverse square law of propagation. Let me discuss Chinese concepts on energy before returning to RPO satellites as a platform for applying such energy.

China's Doctrine Emphasizes Systems, Speed, and Energy

It is well-established now by PLA watchers and PLA doctrine analysts, from authoritative sources like *Science of Military Strategy*, that Chinese strategy emphasizes battlefield control in a multi-dimensional space. The Academy of Military Sciences authors say explicitly that:

> Space and cyberspace increasingly constitute important battlefields after the traditional battlefields of land, sea, and air. A new type of five-dimensional battlespace of land, sea, air, space, and cyber is currently taking shape, which is wide in scope, hyper-dimensional, and combines the tangible and intangible. Battlefield control is moving from control of the land, sea, and air toward control of space and cyber.

[i] The views expressed here are the author's only and do not necessarily reflect the views of any US Government or other entities.

> 继传统的陆、海、空战场之后，太空和网络空间日益成为重要战场，陆、海、空、天、网五维一体的大范围、高立体、有形与无形相交织的新型战场空间正在形成，战场制权由制陆、制海、制空向制天和制网延伸。[4]

But to many PLA analysts, these multi-year coordinated volumes give a rear view perspective of China's strategic thinking. To understand where the thinking is going, we often look to military journals, think pieces, and even blog posts. For instance, in December 2016, an analysis appeared in *National Defense Reference*,[ii] a relatively new publication, in which the author asserts that China can defeat the United States' "network-centric warfare" with "energy-centric warfare":

> "Energy-centric warfare" stresses increasing the speed of the link which is "attack." The specific way to do so is to develop new concept weapons such as near space hypersonic weapons, electromagnetic rail guns, and directed energy weapons, shortening the time between detection and destruction of a target.[5]

The objective of "energy-centric warfare", according to the author, is to apply effects as quickly as the information from the battlefield can be derived or shared, effectively getting inside the adversary's OODA (Observe, Orient, Decide, Act) loop. Taking the doctrine of moving toward a hyper-dimensional battlespace emphasizing space and cyber and this evolving thinking about applying energy-based weapons faster than an adversary can react, the following example given in that same piece is illustrative:

> A high power output microwave transmitter is composed of a super-high powered microwave system, an energy source system, and a large transmission antenna. Its structure is similar to that of a radar transmission system, but its radiated energy is hundreds or even 10,000 times greater than a radar. In actual war, a directed radiation high power output microwave beam can be used to cause disordered logic in a targeted piece of equipment, or even to burn out electronic equipment.[6]

This description of a high-power microwave system is just one example of how China's evolving strategic thinking would make use of directed-energy weapons. Damage and destruction are important effects, but the approach of "systems-of-systems confrontation" (体系对抗) that the PLA has pursued in recent years means that, just as valuable are the effects of degradation, denial, and deception. Hence, I would emphasize the phrase, "disordered logic" in the above quote, indicating the generation of electronic effects in the componentry of the targeted system. This is part of a spectrum of effects that directed energy can have on the targeted system depending on many variables and scenarios. In the cyber world, there is growing appreciation for a cyber-electronic warfare (cyber-EW) spectrum of effects, adding in high-powered directed energy systems extends that spectrum of effects into damage or destruction, but they all reside on a spectrum based on the physics of electromagnetic propagation.

Chinese Research into Counterspace Cyber-EW Effects

Satellites are particularly vulnerable targets for directed energy effects, both because they are comprised of sensitive electronics and because their operations are relatively fragile, meaning any sub-

[ii] An in-depth think-piece magazine that began publication in 2015, published by the Liberation Army Publishing House.

system failure could be potentially mission-ending. Chinese strategic thinking also holds space in high regard, doctrinally, as the proverbial "high ground" for enabling modern operations.[7] Directed energy effects can be delivered against satellites using a variety of devices, including flux compression generators (FCGs), nuclear and non-nuclear electromagnetic pulse, and high-power microwave emitters. Satellite systems are generally designed to be electrically isolated, including building in grounding planes for system components and shielding the satellite chassis from exterior charge. However, as noted in JPL's satellite design handbook, any penetration of the satellite body, such as the star tracker used to orient the satellite, can become an infiltration point for electromagnetic interference.[8] Understanding the weak points of a particular satellite could lead a determined adversary to finding methods for coupling the right frequency and power level necessary to generate electrical effects onboard the satellite. Antennas, including payload, TT&C, and crosslink antennas, are also de facto penetration points into the satellite system.

Researchers in China's academic departments, industrial research institutes, and state key laboratories have been investigating the characteristics of both US Government and commercial satellites to generate effects along the breadth of the cyber-EW spectrum. Over the course of the last decade or so, a body of research has emerged exemplifying the many avenues of research these groups have taken.

- A 2004 paper by researchers at the PLA Electronic Engineering Institute proposed a method for disrupting the Iridium satellite communications constellation by degrading or corrupting inter-satellite datalinks to generate network-wide effects.[9]

- The proposed method of disrupting crosslink data transfer has implications for emerging commercial enterprises that plan for hundreds or thousands of interlinked LEO communications satellites.[10]

- A 2006 paper by another set of researchers at the PLA Electronic Engineering Institute proposed a space-based jammer tailored for use against the anti-jamming features of the Defense Satellite Communications Series III military communications system.[11]

- A 2006 paper by researchers at the National Key Laboratory of Communication proposed a distributed network of pico-satellite jammers, with the advantages of reducing power requirements exponentially and accessing the target antenna's main lobe, which is usually less protected than antenna side lobes.[12]

- A 2007 paper by researchers from the National Key Laboratory of Anti-Jamming Communication Technology and the University of Electronic Science and Technology describes the advantages of using a network of micro-satellite jammers over a ground-based jammer to include the orders of magnitude improvement in signal-to-jamming power ratios from 10 m away versus 1,000 km, and the potential to jam the target undetected.[13]

- A 2009 paper by researchers at Xidian University's State Key Laboratory for Wide Band Gap Semiconductor Materials and Devices proposed using an electromagnetic pulse device to damage low-noise amplifiers, a common component in satellite antenna subsystems.[14]

- A 2012 paper by authors from the 36th Research Institute of the China Electronic Technology Group Corporation (CETC) proposed overcoming the high power requirements for jamming US

millimeter wave (MMW) satellite communications by using space-based jammers hosted on small satellites, in a "David versus Goliath" attack.[15]

- The authors noted that reducing that distance with a small satellite platform would decrease the power requirements exponentially, and identified potentially susceptible USG assets as the AEHF (Advanced Extremely High Frequency), WGS (Worldwide Global Satcom), and GBS (Global Broadcast Service) satellite constellations.[16]

- The same authors proposed to use cyber-EW means to gain access to TT&C channels for exploitation purposes: "If we are in control of the format of the command and control information, we will be able to interpret such information. As a result, we can acquire additional information such as target address called by a user, the allocated traffic channel, and data encryption scheme adopted."[17]

A related track of research in China focuses on the software and firmware of aerospace platforms, specifically in producing and defending against voltage anomalies, also known as fault injection attacks. These are also known as "glitch attacks," "single event effects," "single event transients," and "single event upsets," all referring to the introduction of voltage differentials that interfere with the normal operation of a given system. Such research is standard practice for any spacefaring nation interested in preserving satellite reliability, though research in a defensive capability often also necessitates development of an offensive correlate.

- A 2005 study by researchers at the China Aerospace Science and Technology Corporation's (CASC) 771 Research Institute in collaboration with academics at the Harbin Institute of Technology created a software-based tool for testing fault injection attacks against "onboard systems" such as processors and memory.[18]

- The same research group had also shown in 2006 that fault injection attacks against aircraft electronic components were more successful against processors than against memory areas.[19]

- In a 2010 study, a group of researchers, including those from the Harbin Institute of Technology and Beihang University conducted fault injection testing against a commercially available aerospace operating system, VxWorks, used in many civil US Government programs.[20]

- A 2012 paper written by researchers from the Beijing Aerospace Automatic Control Institute conducted multi-layer fault injection analysis against a popular civil and military satellite bus standard, the MIL-STD-1553B bus type. They found specific vulnerabilities via their fault injection testing in the "physical layer, electrical layer, and protocol layer" of the standard.[21]

The suite of research examined here gives a sense of the foundational knowledge Chinese space systems researchers already possess, should a decision be made to pursue a cyber-EW counterspace weapons R&D program. The difference between directed energy jamming and damaging a target is a question of amplitude. From this body of research, it is clear that a more sophisticated application of directed energy could generate electrical coupling effects in antennas, penetrations, or ports to deliver cyber-like effects against a satellite. These applications should also be a part of discussions on directed energy and advanced weapons.

Conclusion and Outlook

The primary obstacles to implementing a cyber-EW directed energy weapon against satellites are distance and knowledge. An attacker from the ground would need to transmit exceedingly high power levels, and even then, the effects would be broad and indiscriminate. Using an RPO-enabled satellite as a platform for cyber-EW electromagnetic transmission addresses the power issue via the inverse square law of propagation and also, depending on the distance, allows for more finely tuned attacks on subsystems of the satellite. The other obstacle for an attacker is having exquisite knowledge of the satellite's design and operation. As exceedingly complicated and redundant systems-of-systems, satellites can be said to rely on "security through obscurity" as a first line of defense, that is to say, the protocols and procedures of operating the satellite are not generally readily available to the public. However, this makes such information highly desirable from a state or corporate espionage perspective.

Despite the focus of my overview on Chinese counterspace cyber-EW research, cyber-EW counterspace does not stand alone. It should be considered as one tool in the quiver of a "combined arms" counterspace campaign. For instance, a glitch attack conducted on a pass maneuver by a "rendezvous and cyber operations" satellite may on its own be temporary, but combined with a more traditional jamming attack against the satellite's TT&C channel, it could be mission-ending for the victim. As China exhibits increasingly advanced RPO capabilities, analysts should be on the lookout for more evidence of the development and deployment of a "rendezvous and cyber operations" satellite. Such a satellite could prove to be a novel platform for delivering cyber-EW effects against high-value space assets.

Let me end on a hopeful note. Diplomatic and political engagement with China may help clarify intent with regard to developing such types of space-based capabilities, and establish bilateral norms for space cyber-EW behavior, which would be mutually beneficial. Recall, not so long ago, that a period of relatively constructive bilateral relations in 2014-2015 led to agreements on cyber, climate change, and de-ratcheting of Taiwan Strait and other maritime issues. Diplomatic and political engagement could be constructive in regards to emerging technologies in space, as well.

Table 1. Chinese RPO Missions

Program	Launched	Description
Banfei Xiaoweixing-1	2008	BX-1 was deployed from the orbital module of Shenzhou-7 and relayed images of the main vessel while flying in co-orbital formation.[22]
Shijian-12	2010	SJ-12 maneuvered within 27 km of SJ-6F two months after launch, then made a series of maneuvers to within 300 m distance, causing a likely low-speed contact resulting in orbital perturbations observed from the ground.[23]
Shiyan-7	2013	Rendezvoused with CX-3 and SJ-7, probable deployment of robotic arm.[24]
Tianyuan-1	2016	Satellite servicing/refueling experiment that transferred 60 kg of fuel while in orbit.[25]
Aolong-1	2016	Experimental robotic manipulator payload for orbital debris mitigation.[26]

Banfei Xiaoweixing-2	2016	A second BX was launched from the Tiangong-2 space station as part of the Shenzhou-11 manned mission in October 2016.[27]
Shijian-17	2016	Suspected GEO belt inspection or signals intelligence satellite.[28]

[1] Dong Feng, "Tiangong 2 launched into orbit by CZ-2F," China Space Report, 15 September 2016, <https://chinaspacereport.com/2016/09/15/tiangong-2-launched-into-orbit-by-cz-2f/> (Accessed 18 October 2016).

[2] "SCMP: Is China Militarising Space? Experts Say New Junk Collector Could Be Used As Anti Satellite Weapon," *South China Morning Post*, <http://www.scmp.com/news/china/diplomacy-defence/article/1982526/china-militarising-space-experts-say-new-junk-collector> (Accessed 12 September 2016).

[3] "In-Space Eavesdropping? – China's Shijian-17 completes High-Altitude Link-Up," Spaceflight101.com, 9 December 2016, < http://spaceflight101.com/cz-5-maiden-flight/shijian-17-rendezvous-with-chinasat-5a/> (Accessed 13 February 2017).

[4] *The Science of Military Strategy*, Military Science Publishing House, 2013, p. 96.

[5] Lan Shunzheng, "New Concept for Future War—'Big Energy-centric Warfare'", *National Defense Reference*, 27 December 2016, <http://mini.eastday.com/a/161228110024337.html> (Accessed 13 February 2017).

[6] *Ibid*.

[7] Dean Cheng, written testimony, U.S.-China Economic and Security Review Commission, Hearing on China's Space and Counterspace Programs, 18 February 2015.

[8] Henry B. Garrett and Albert C. Whittlesey, *Guide to Mitigating Spacecraft Charging Effects*, Hoboken, NJ: John Wiley & Sons, Inc., 4 May 2012, p. 35.

[9] Zhao Haiyan, Cheng Pengjun, Shi Yingchun, "Introduction of Key Technologies in LEO Satellites Communications and EM Threat," *Aerospace Electronic Warfare*, March 2004.

[10] Amy Svitak, "SpaceX, OneWeb Unveil Rival Broadband Constellation Plans," *Aviation* Week, 21 January 2015, <http://aviationweek.com/space/spacex-oneweb-unveil-rival-broadband-constellation-plans> (Accessed 10 October 2016).

[11] Xu Xiaofeng, Zhu Xiaosong, Liu Liyuan, "Jamming Analysis Based on a Certain Satellite Communication System," *Aerospace Electronic Warfare*, October 2006, pp. 28-29, 45.

[12] Xiao Yuxiang, Zhou Wenjiong, Zhu Lidong, Wu Shiqi, "Distributed Jamming System and its Key Technologies Based on Pico-Satellite," *Aerospace Electronic Warfare*, October 2006, pp. 25-27.

[13] Zhou Wenjiong, Xiao Yuxiang, Zhu Lidong, Wu Shiqi, "Delay Analysis of Micro-Satellite Based Repeater Deception Jamming," *Electronic Information Warfare Technology*, November 2006, pp. 27-30.

[14] Xi Xiaowen, Chai Changchun, Ren Xingrong, Yang Yintang, Zhang Bing, "Transient Response of Bipolar Transistor under Intense Electromagnetic Pulse on Collector," IEEE Proceedings of 16th IFPA, 2009, <http://ieeexplore.ieee.org/iel5/5210717/5232547/05232611.pdf> (Accessed 27 November 2016).

[15] Lin Jinshun, Wu Xianzhong, Lu Shengjun, Jiang Chunshan, "Countermeasure Technology for MMW Satellite Links," *Aerospace Electronic Warfare*, October 2012, pp. 20-22.

[16] *Ibid*.

[17] *Ibid*.

[18] Peng Junjie, Huang Qingcheng, Hong Bingrong, Li Rui, Yuan Chengjun, "A Software Fault Injection Tool for Evaluation of Dependability of Onboard System," *Journal of Astronautics*, November 2005, pp. 823-827.

[19] Peng Junjie, Huang Qingcheng, Hong Bingrong, Li Rui, Yuan Chengjun, Wei Zhenhua, "Test Fault Sensitivity of a Digital Processor by a Pure Software Approach," *Journal of Astronautics*, January 2006, pp. 108-112.

[20] Wang Xinsheng, Huang Zhenyuan, Liang Bin, "A Software-Implemented Fault Injection Method for Onboard Computer Based on VxWorks," *Aerospace Control*, October 2010, pp. 84-88.

[21] Lian Meng, Li Xuefeng, "Design and Research of Fault Injection on 1553B Bus," *Aerospace Control*, April 2012, pp. 84-88.

[22] Peter R. Bond, ed., *Jane's Space Systems and Industry 2011-2012*, Alexandria, VA: IHS Global Limited, 2011, p. 536.

[23] Peter R. Bond, ed., *Jane's Space Systems and Industry 2011-2012*, Alexandria, VA: IHS Global Limited, 2011, p. 588.

[24] Marcia S. Smith, "Surprise Chinese Satellite Maneuvers Mystify Western Experts," SpacePolicyOnline, 19 August 2013, <http://www.spacepolicyonline.com/news/surprise-chinese-satelllite-maneuvers-mystify-western-experts> (Accessed 14 September 2016).

[25] Jeffrey Lin, PW Singer, "China's Largest Space Launch Vehicle Long March 7 Flies With Technological Triple Whammy," *Popular Science*, 8 July 2016, <http://www.popsci.com/chinas-largest-space-launch-vehicle-long-march-7-flies-with-technological-triple-whammy> (Accessed 18 October 2016).

[26] "SCMP: Is China Militarising Space? Experts Say New Junk Collector Could Be Used As Anti Satellite Weapon," *South China Morning Post*, <http://www.scmp.com/news/china/diplomacy-defence/article/1982526/china-militarising-space-experts-say-new-junk-collector> (Accessed 12 September 2016).

[27] "Companion Satellite released from Tiangong-2 Space Lab for Orbital Photo Shoot," Spaceflight101.com, 23 October 2016, <http://spaceflight101.com/tiangong-2/companion-satellite-released-from-tiangong-2/> (Accessed 14 February 2017).

[28] "In-Space Eavesdropping? – China's Shijian-17 completes High-Altitude Link-Up," Spaceflight101.com, 9 December 2016, < http://spaceflight101.com/cz-5-maiden-flight/shijian-17-rendezvous-with-chinasat-5a/> (Accessed 13 February 2017).