Études de l'Ifri

Proliferation Papers 62

CURRENT AND FUTURE TRENDS IN CHINESE COUNTERSPACE CAPABILITIES

Brian WEEDEN

November 2020

ifri since 1979

Security Studies Center

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0265-6

How to cite this publication:
Brian Weeden, "Current and Future Trends in Chinese Counterspace Capabilities", *Proliferation Papers*, Ifri, November 2020.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Dr. Brian Weeden is the Director of Program Planning for Secure World Foundation and has more than 20 years of professional experience in space operations and policy.

Dr. Weeden directs strategic planning for future-year projects to meet the Foundation's goals and objectives, and conducts research on space sustainability issues. He is a member and former Chair of the World Economic Forum's Council on the Future of Space Technologies, a former member of the Advisory Committee on Commercial Remote Sensing (ACCRES) to the National Oceanic and Atmospheric Administration (NOAA), and the Executive Director of the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS). Prior to joining SWF, Dr. Weeden served nine years on active duty as an officer in the United States Air Force working in space and intercontinental ballistic missile (ICBM) operations.

Dr. Weeden holds a Bachelor's Degree in Electrical Engineering from Clarkson University, a Master's Degree in Space Studies from the University of North Dakota, and a Ph.D. in Public Policy and Public Administration from George Washington University in the field of Science and Technology Policy.

Editorial board

Abstract

China is in the midst of a long-term effort to develop a world-class space program with a strong military and national security component. Since 2015, Chinese official and unofficial writings have increasingly emphasized the importance of space warfare, including for offensive and coercive uses. In parallel, China has engaged in a significant and dedicated effort to develop a wide array of destructive and non-destructive offensive counterspace capabilities since the early 2000s, some of which are – or soon will become – operational. This study explores the multiple areas of Chinese counterspace capability developments, from co-orbital rendezvous operations to direct ascent antisatellite interceptors and electronic and cyber warfare. It summarizes what is known about current programs, offers estimates regarding the unique characteristics of each capability area and how advanced Chinese capabilities are in each field. While China's search for a large array of counterspace capabilities is not unique, it could both directly and indirectly affect U.S. and European strategic interests and thus has vast implications for transatlantic security.

Résumé

La Chine a engagé un effort de long terme en vue de développer un programme spatial de premier ordre, comportant une forte composante consacrée à la sécurité nationale et au domaine militaire. Depuis le début des années 2000, la Chine investit significativement dans le développement d'un large spectre de capacités antisatellites destructives et non destructives, dont certaines sont – ou seront bientôt – opérationnelles. Plus récemment, un nombre grandissant d'écrits officiels et non officiels chinois a souligné l'importance de l'action militaire dans l'espace, y compris à des fins offensives et coercitives. Cette étude explore l'ensemble des programmes chinois de lutte dans l'espace, qu'il s'agisse des capacités d'action co-orbitale, de missiles antisatellites à ascension directe ou de moyens de guerre cybernétique et électronique visant les systèmes spatiaux. L'étude s'appuie sur l'ensemble des données connues sur les programmes existants, évalue les caractéristiques propres à chaque système et le degré d'avancement chinois en la matière. L'ampleur de l'effort investi par la Chine dans l'acquisition d'une large gamme de capacités de lutte dans l'espace n'est pas unique. Néanmoins, il est susceptible d'affecter – tant directement qu'indirectement – les intérêts stratégiques américains et européens, et a ainsi d'importantes implications pour la sécurité transatlantique.

Table of Contents

INTRODUCTION 11

COUNTERSPACE POLICY, DOCTRINE AND ORGANIZATION 15

CHINESE COUNTERSPACE EFFORTS 17

- Co-orbital ASAT 18
- Direct Ascent ASAT 23
- Electronic Warfare 28
- Directed Energy 30
- Cyber 33
- Space Situational Awareness 34

IMPLICATIONS FOR EUROPE AND TRANSATLANTIC SECURITY 39

Introduction

Outer space has been used for national security capabilities since the dawn of the Space Age in the 1950s. From the very beginning, the two original space powers, the United States and the Soviet Union, saw outer space as a potential source of military and intelligence benefits. The Eisenhower Administration declared space-based intelligence collection to be among the highest national priorities in 1961.[1] Although the Outer Space Treaty of 1967 placed strict limits on military bases, training, and weapons deployment on celestial bodies and placement of weapons of mass destruction in orbit, the treaty explicitly allowed for "peaceful uses of outer space" that included many activities beneficial to national security.[2] Over the next thirty years, both superpowers deployed space-based assets that provided their militaries with reconnaissance, intelligence, surveillance, communications, navigation, targeting, weather, and other essential capabilities.

The growth of military space capabilities also drove the development of offensive counterspace capabilities that could be used to deny an adversary the use of space during a conflict. The most well-known offensive counterspace capabilities are anti-satellite weapons (ASATs) that can destroy satellites. The first known ASAT test was conducted by the United States in September 1959, less than one year after the Soviets launched the first satellite, Sputnik, into orbit. An air-launched ballistic missile from the High Virgo program was modified to be able to track and target a satellite, but the telemetry signal was lost, and the test was ultimately inconclusive.[3] Over the course of the next forty years, the United States and Soviet Union conducted nearly 50 ASAT tests of various types, some of which became operationally deployed systems.[4]

---

1. National Security Council, "Certain Aspects of Missile and Space Programs", Washington, DC, January 18, 1961, available at: https://aerospace.csis.org.
2. B. Cheng, "Properly Speaking, Only Celestial Bodies Have Been Reserved for Use Exclusively for Peaceful (Non ... Military) Purposes, but Not Outer Void Space", *International Law Studies*, Vol. 75, pp. 81-117.
3. A. Parsch, "WS-199", *Designation-Systems.Net*, November 1, 2005, available at: www.designation-systems.net.
4. A summary of all known ASAT tests in space can be found in B. Weeden and K. Pfrang, "History of ASAT Tests in Space", Secure World Foundation, updated August 6, 2020, available at: https://docs.google.com.

Although both the United States and Soviet Union possessed ASAT capabilities, there are no known examples of destructive ASATs being used in a hostile manner. This was likely due to the close links between satellites and nuclear war; the United States in particular relied on satellites as a key element of its strategic nuclear warning network. Some of the bilateral nuclear arms control agreements, such as the Strategic Arms Limitation Talks (SALT I) treaty signed in 1972, included specific prohibitions on interference with "national technical means," a euphemism for space-based verification capabilities.[5]

After the collapse of the Soviet Union in the early 1990s, counterspace capabilities became less of a concern. While the United States continued some basic research and development, its focus shifted to improving and integrating space capabilities that can enhance conventional warfighting. Beginning with Operation Desert Storm and the NATO campaign in Kosovo in the 1990s, the United States military showed just how much more effective conventional military warfare can be when enhanced by space capabilities, such as by enabled precision guided munitions (PGMs).[6] This effectiveness came to a peak with the wars in Afghanistan and Iraq following the events of 9/11/2001, where the U.S military leveraged space capabilities to an incredible degree. For example, many uncrewed aerial vehicles (UAVs) operations rely entirely on satellites for navigation, routing of command and control signals, and routing of data feeds.[7] Other countries have followed suit and begun integrating space capabilities into their own conventional militaries, although none have done so to the same extent as the United States.

The emergence of space as a key contributor to conventional warfighting and military operations is a significant change from the Cold War era. For much of the Cold War, space was limited to mainly a strategic role in collecting strategic intelligence, enforcing arms control treaties, and warning of potential nuclear attack. The increased asymmetric reliance on and use of some of those same strategic space capabilities and newer tactical space capabilities to directly support conventional warfighting has increased the incentives for countries to develop offensive counterspace capabilities, while also decreasing the deterrent value of the nuclear link.[8] Since 2005, China, Russia, the United States, and India have conducted more than 20

5. "Strategic Arms Limitation Talks (SALT I)", *Nuclear Threat Initiative*, updated October 26, 2011, available at: https://www.nti.org/learn.
6. B. Lambeth, "Accomplishments of the Air War", in B. Lambeth (ed.), *NATO'S Air War for Kosovo: A Strategic and Operational Assessment*, Santa Monica, CA: RAND Corporation, 2001.
7. A. Cuadra and C. Whitlock, "How Drones are Controlled", *The Washington Post*, June 20, 2014.
8. B. Weeden and V. Samson (eds.), *Global Counterspace Capabilities: An Open Source Assessment*, Washington, DC: Secure World Foundation, April 2020.

additional ASAT tests in space,[9] signaling a renewed interest in counterspace capabilities as part of military capabilities for future conflicts.

China is currently in the midst of a long-term effort to develop a world-class space program. As noted in a recent report from CNA, Beijing has set significant goals for growing China's space program over the next thirty years as part of achieving the "China Dream" to make China stronger and more prosperous.[10] China's space development effort encompasses major efforts in space science and human space exploration, civil capabilities to provide social and economic benefits, and a strong military and national security component. The following sections provide more details on Chinese policy, doctrine, and organization of counterspace capabilities and then a detailed assessment of the different technology areas. Note that China's policy and doctrine on counterspace capabilities has evolved in parallel with the development of the technologies themselves.

9. *Ibid.*
10. K. Pollpeter *et al.*, *China's Space Narrative*, Montgomery, AL: China Aerospace Studies Institute, September 2020.

Counterspace Policy, Doctrine and Organization

China's official public statements on space warfare and space weapons have consistently adhered to the principle of the use of outer space for peaceful purposes and opposed to the weaponization of or an arms race in outer space.[11] However, since 2015, other official writings suggest China's position on space warfare and space weapons has become more nuanced. China's 2015 defense white paper, China's Military Strategy, for the first-time designated outer space as a military domain and linked developments in the international security situation to defending China's interests in space. The defense white paper states that "Outer space has become a commanding height in international strategic competition. Countries concerned are developing their space forces and instruments, and the first signs of weaponization of outer space have appeared." More recent research has concluded that a major rationale for China's space program is to help make the country stronger, including its ability to project power far from its shores and defeat technologically advanced adversaries such as the United States.[12]

Chinese analysts argue that China must develop counterspace weapons to balance U.S. military superiority and protect China's own interests.[13] As one researcher writes, China's development of ASAT weapons is to protect its own national security and adds that "only by preparing for war can you avoid war."[14] The authors of the 2013 Science of Military Strategy write that given the wide-range of rapid strike methods, "especially space and cyber

11. Permanent Mission of the People's Republic of China to the UN, "Statement by Ms. Pan Kun of the Chinese Delegation at the 71st Session of the UN General Assembly on Agenda Item 48: International Cooperation in the Peaceful Uses of Outer Space", October 13, 2016, available at: www.china-un.org.
12. K. Pollpeter *et al.*, "China's Space Narrative: Examining the Portrayal of the U.S.-China Space Relationship in Chinese Sources and its Implications for the United States", *op. cit.*, p. 55.
13. X. Nengwu and H. Changyun, "Space Deterrence: Changes in the U.S. Strategic Deterrence System and Global Strategic Stability" (太空威慑: 美国战略威慑体系调整与全球战略稳定性), *Foreign Affairs Review* (外交评论), No. 5, 2014, p. 62; X. Lei, Q. Mu and W. Qu, "Who Stirs Up a Space War?" (谁在挑起太空战争？), *Decision & Information* (决策与信息), Vol. 2, No. 339, 2013, p. 18; Y. Caixia and A. Dun, "On the Legality of the Development of ASATs for China" (论中国发展反卫星武器的合法性), *Journal of Journal of Beijing University of Aeronautics and Astronautics* (Social Sciences Edition) (北京航空航天大学学报（社会科学版）), Vol. 23, No. 2, March 2010, pp. 46, 47, 50.
14. J. Yu, "Space Thunder: Development of Hard-Kill Antimissile Weapon and China's Antimissile Testing" (太空惊雷 反导硬杀伤武器的发展及中国反导试验), *Shipborne Weapons* (舰载武器), No. 2, 2010, p. 14.

attack and defense methods," China must prepare for an enemy to attack from all domains, including space.[15]

In addition to actual warfighting, space power can also be used to coerce. Chinese analysts write that having the ability to destroy or disable an opponent's satellites may deter an adversary from conducting counterspace operations against Chinese satellites. Space power can also improve the overall capabilities of a military and serve as a deterrent force not just against the use of specific types of weapons, but also as a general capability that can deter a country from even becoming involved in a conflict.[16]

Chinese military writings overall place a heavy emphasis on gaining the initiative at the outset of a conflict, including during the deployment stage. Looking at the 1991 Gulf War, and the initial invasions of Afghanistan in 2001 and Iraq in 2003, Chinese military analysts assess that the PLA cannot allow the U.S. military to become fully prepared lest they cede victory. According to the authors of Study of Space Operations, China will "do all it can at the strategic level to avoid firing the first shot,"[17] but recommend that China should "strive to attack first at the campaign and tactical levels in order to maintain the space battlefield initiative."[18] They also argue that fighting a quick war is one of the "special characteristics of space operations" and that a military should "conceal the concentration of its forces and make a decisive large-scale first strike."[19]

In recent years, China has undertaken significant reorganization of its military space and counterspace forces. In 2016, Chinese President Xi Jinping initiated a sweeping reorganization of the PLA. Part of this reorganization included the creation of the Strategic Support Force (SSF) as the fifth military service by merging existing space, cyber and electronic warfare units under a new unified command that reports directly to the Central Military Commission. The intent is to shift the PLA's most strategic, informatized missions from a discipline-centric to domain-centric force structure and enable full-spectrum war-fighting.[20] The space elements of the SSF include space launch, support, TT&C, and ISR. At this point, it is unclear if the SSF also has authority for kinetic ASAT attacks or whether that remains with the PLA Rocket Force.[21]

15. "The Science of Military Strategy", Beijing: Military Science Publishing House, 2013, p. 102.
16. J. Lianju and W. Liwen (eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing: Military Science Publishing House, 2013, p.127.
17. *Ibid.*, p. 42.
18. *Ibid.*, p. 52.
19. *Ibid.*, pp. 142-143.
20. J. Costello, "The Strategic Support Force: Update and Overview", *China Brief*, Vol. 13, No. 19, December 21, 2018.
21. *Ibid.*

Chinese Counterspace Efforts

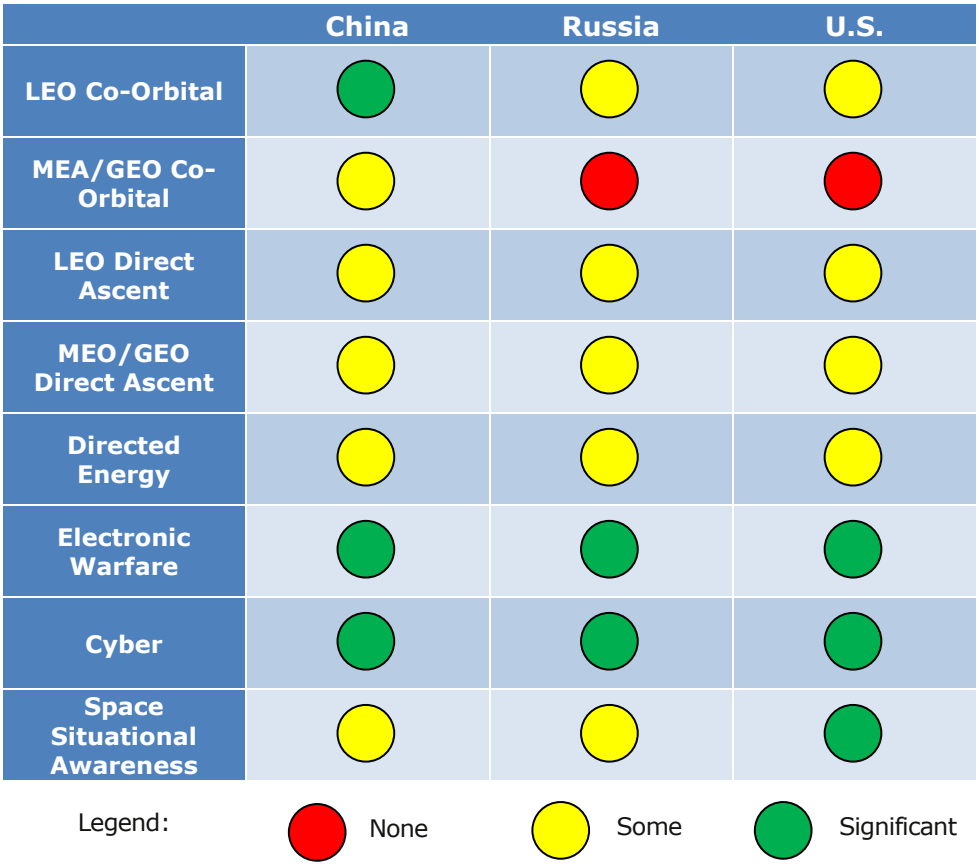
China sees counterspace capabilities as a key part of its national security, particularly in the emerging competition with the United States. Having observed the conventional warfighting effectiveness of the United States military in Iraq, Kosovo, Afghanistan, and Iraq again, the Chinese People's Liberation Army has concluded that it must be able to deny the United States the use of space in order to deter or win a potential future conflict. As such, China has engaged in a significant and dedicated effort to develop a wide array of destructive and non-destructive offensive counterspace capabilities since the early 2000s, some of which are currently becoming or soon will become operational. Chinese counterspace capabilities can be broken down into the following categories:

- **Co-orbital:** weapons that are placed into orbit and then maneuver to approach the target and can disable, damage or destroy it through a variety of means
- **Direct Ascent:** weapons that use ground, air-, or sea-launched missiles with interceptors (kill vehicles) that are used to kinetically destroy satellites through a hypervelocity impact, but are not placed into orbit themselves
- **Directed Energy:** weapons that use focused energy, such as laser, particle, or microwave beams to interfere with or destroy space systems
- **Electronic Warfare:** weapons that use radiofrequency energy to interfere with or jam the communications to or from satellites
- **Cyber:** weapons that use software and network techniques to compromise, control, interfere, or destroy computer systems
- **Space Situational Awareness (SSA):** knowledge about the space environment and human space activities and generally includes detection, tracking and characterization of space objects and space weather monitoring and prediction. While SSA is not uniquely used for counterspace, it is a critical enabler for both offensive and defensive counterspace operations.[22]

22. There is a shift by some militaries to rename this category to Space Domain Awareness (SDA) to reflect a focus on SSA for space warfighting. As SSA remains in use for the broader set of capabilities and is used by more countries, this article will use SSA throughout. See S. Erwin, "Air Force: SSA is no more; it's 'Space Domain Awareness'", *Spacenews*, November 14, 2019, available at: https://spacenews.com.

China's overall capabilities in these areas are assessed in Figure 1 in comparison to those of Russia and the United States.

Figure 1: Overall assessment of Chinese, Russian, and American counterspace capabilities



The following sections detail what is currently known about China's development of offensive counterspace capabilities, based on open source reporting and information. The sections are broken down according to the aforementioned categories. Each section contains a summary of China's current capabilities, on-going research and development, and potential military utility in that category and concludes with an estimate of how China's capabilities in that area might develop in the future.

Co-orbital ASAT

Co-orbital ASATs place an interceptor into orbit, which then maneuvers to alter its orbit to a trajectory that brings it close to a target. Co-orbital ASATs can maneuver to approach immediately after being placed into orbit or after remaining dormant for an extended period of time. They can try to damage or destroy their target by a variety of means, including direct collision at

hyper velocities, releasing a cloud of fragments that will collide with the target, using a robotic arm to damage or remove parts of a target satellite, or using electronic warfare or directed energy weapons at close range. Regardless of the technique used, co-orbital ASATs require onboard guidance, navigation, and control systems to identify and track a targeted space object and fine-tune their trajectory for close approach and interception.

To date, there is no concrete public proof that China has tested a co-orbital ASAT or has an official program underway to develop one.[23] However, China has conducted multiple tests of rendezvous and proximity operations (RPO) technologies in both low Earth orbit (LEO) and geosynchronous Earth orbit (GEO) regions that could be used as the basis for a future co-orbital ASAT capability.[24]

The first known Chinese robotic RPO in LEO occurred in September of 2008 when the Chinese human spaceflight mission Shenzhou 7 deployed a small satellite to practice RPO capabilities.[25] That was followed in the summer of 2010 with a satellite called the SJ-12 that conducted a series of close approaches with another Chinese satellite, the SJ-6F, which was placed into orbit on the same launch.[26] The close approaches took place over a period of weeks and occurred at very low relative orbital velocities with the closest approach being within 300 meters. There is evidence that the SJ-12 "bumped" into the SJ-6F during one of the approaches, although it was at only a few meters per second speed and neither satellite appeared damaged by the incident, nor was there any release of orbital debris.

A more complicated Chinese RPO demonstration in LEO occurred in 2013. Three satellites (SY-7, CX-3, and SJ-15) were placed into orbit on the same launch.[27] In August 2013, the SJ-15 conducted a series of RPO with the CX-3 within a few kilometers and with the SJ-7, a Chinese satellite launched

23. Russia is the only country known to have a dedicated co-orbital ASAT program that was tested from 1963-1994 and may have recently been reactivated. See K. Pfrang and B. Weeden, "Russian Co-Orbital Anti-Satellite Testing", *Fact Sheet*, Secure World Foundation, August 2020. The United States has conducted a co-orbital intercept as part of a missile defense test, but there is no public evidence of a formal development program. See K. Pfrang and B. Weeden, "U.S. Co-Orbital Anti-Satellite Testing", *Fact Sheet*, Secure World Foundation, August 2020.

24. RPO technologies have been routinely used for human spaceflight missions since the 1960s and can also be used to support beneficial missions such as on-orbit inspections, refueling, assembly, repositioning, and removal of orbital debris.

25. U.S.-China Economic Security Review Commission, "2019 Annual Report to Congress", November 2019.

26. A more detailed technical analysis of this event can be found in B. Weeden, "Dancing in the Dark; The Orbital Rendezvous of SJ-12 and SJ06F", *The Space Review*, August 30, 2010, available at: www.thespacereview.com.

27. J. McDowell, posting on the *NASAspaceflight.com* forums, July 20, 2013, available at: http://forum.nasaspaceflight.com.

in 2007. The SJ-15 did another RPO with SJ-7 in May 2014. Separately, the SY-7, which was reported to have a tele-operated robotic arm, released a small satellite that orbited within close proximity of SY-7 for several days. Some reports claim that the arm was used to dock the subsatellite, but the publicly available tracking data was not precise enough to verify that claim.[28]

Another Chinese launch in 2016 was widely reported to include an RPO and robotic arm capture in LEO but in reality did not. The Aolong-1, also known as the Advanced Debris Removal Vehicle (ADRV) or "Roaming Dragon," was a small satellite developed by Harbin Institute of Technology under contract to CALT to reportedly demonstrate using a robotic arm to capture a small piece of space debris for removal from orbit.[29] It was placed into orbit in June 2016, however it never approached or rendezvoused with any other objects during its short two months in orbit.

China has also conducted robotic RPO demonstrations in GEO. In November 2016, China placed the SJ-17 satellite in GEO, which was publicly declared to be testing advanced technologies. Several days after reaching GEO, the SJ-17 began maneuvering to place itself into the active GEO belt close to another Chinese satellite, Chinasat 5A.[30] The SJ-17 made several small maneuvers to circumnavigate Chinasat 5A at a distance of between 50 and 100 km for several days, slowly closing in to within a few kilometers on November 30, and then returning to a 50 to 100 km standoff distance. They separated again in December 2016, after which the SJ-17 drifted first eastward and then westward along the geostationary belt until March 2018. Over the next few months, the SJ-17 conducted a complex series of energy-intensive maneuvers to rendezvous with Chinasat 1C, a Chinese communications satellite launched in December 2015 that had apparently experienced a recent anomaly. After the rendezvous, Chinasat 1C moved back to its operational location, which suggests the SJ-17 was used to inspect Chinasat 1C to determine the source of the anomaly and then monitor the recovery attempt.

28. For a more detailed analysis of these evenglots, see B. Weeden and V. Samson, *Global Counterspace Capabilities: An Open Source Assessment*, *op. cit.*, pp. 2-3.
29. "China Lands Prototype Crew Spacecraft after Inaugural Long March 7 Launch", *Spaceflight101*, June 27, 2016, available at: http://spaceflight101.com.
30. B. Hall, "Ep16 – Chinasat 1C Space Activities", *Analytical Graphics, Inc.*, July 2, 2019, available at: www.youtube.com.

Table 1 - Recent Chinese Rendezvous and Proximity Operations

Date(s)	System(s)	Orbital Parameters	Notes
June – Aug. 2010	SJ-O6F, SJ-12	570-600 km; 97.6°	SJ-12 maneuvered to rendezvous with SJ-06F. Satellites may have bumped into each other.
July 2013 – May 2016	SY-7, CX-3, SJ-15	Approx. 670 km; 98°	SY-7 released an additional object that it performed maneuvers with and may have had a telerobotic arm. CX-3 performed optical surveillance of other in-space objects. SJ-15 Demonstrated altitude and inclination changes to approach other satellites.
Nov. 2016 – Feb. 2018	SJ-17, YZ-2 upper stage	35,600 km; 0°	YZ-2 upper stage failed to burn to the graveyard orbit and stayed near GEO. SJ-17 demonstrated maneuverability around the GEO belt and circumnavigated Chinasat 5A.
Jan. 2019	TJS-3, TJS-3 AGM	35,600 km; 0°	TJS-3 AKM separated from the TJS-3 in the GEO belt and both performed small maneuvers to maintain relatively close orbital slots.

The activities of the SJ-12, SJ-15, and SJ-17 are more consistent with the demonstration of RPO technologies for the purpose of satellite servicing, space situational awareness, and inspection than those of co-orbital ASAT testing. Their operational pattern was consistent with slow, methodical, and careful approaches to rendezvous with other space objects in similar orbits instead of sudden, high relative velocity approaches seen in destructive collisions. Notably, a counterspace assessment released by the Defense Intelligence Agency (DIA) in February 2019 stated that China is developing capabilities for inspection, repair, and space debris removal that may also be used as a weapon but did not specifically state that any of these Chinese RPO activities was a weapons test.[31]

These Chinese RPO demonstrations also appear to mirror historical and current U.S., Russian, and European RPO testing and activities. Specifically, they appear similar in nature to the activities of the U.S. Air Force's XSS-11 satellite, which was used to do inspections of satellites in LEO in 2005 and 2006;[32] DARPA's OrbitalExpress satellite, which launched as a

31. "Challenges to Security in Space", Defense Intelligence Agency, Report, Washington, DC., January 2019.

32. T. M. Davis and D. Melanson, *Xss-10 Micro-Satellite Flight Demonstration*, Atlanta, GA: Georgia Institute of Technology, November 10, 2005.

joined pair and conducted a series of rendezvous, docking, and robotic arm experiments in 2007;[33] the Swedish Mango and Tango cubesats that were part of the Prototype Research Instruments and Space Mission technology Advancement (PRISMA) mission, which demonstrated cooperative rendezvous and proximity operations and formation flying in 2010;[34] and the U.S. Air Force's Micro-satellite Technology Experiment (MiTEx) satellites and Geosynchronous Space Situational Awareness (GSSAP) satellites, which conducted inspections in the GEO belt in 2009[35] and 2016.[36] They are also similarly to several recent Russian demonstrations of RPO activities in both LEO and GEO.[37]

There is significant concern within the United States military, however, that China may use these RPO capabilities for an offensive counterspace role in the future. One potential offensive use would be to use the RPO capability get a radio-frequency jammer close to a satellite, thereby greatly amplifying its ability to interfere with the satellite's communications. Another possibility could be to use high power microwaves or lasers from the RPO satellite to interfere with the systems of the target satellite, although these would require significant electrical power that is unlikely to be provided by a small satellite at this time. While possible, to date there is no direct public evidence of such systems being tested on orbit, although there have been multiple research articles published in Chinese journals discussing and evaluating the concept.

The onboard tracking and guidance systems used for rendezvous could be used to try and physically collide with another satellite to damage or destroy it. However, the approach would have to involve much higher relative velocities than what the Chinese RPO satellites have demonstrated to date, and potentially involving higher velocities and longer closing distances than what these satellites are capable of. It is also possible for an RPO system to create "shrapnel"[38] or use electronic warfare or directed energy weapons from close range. Furthermore, the deliberate maneuvering to create a conjunction with the target satellite would be detectable with existing processes already in place to detect accidental close approaches.

33. Lt Col Fred Kennedy, "Orbital Express Space Operations Architecture", *DARPA Tactical Technology Office*, available at: http://archive.darpa.mil.
34. "Prisma", *OHB Sweden*, available at: www.ohb-sweden.se.
35. C. Covault, "Secret Inspection Satellites Boost Space Intelligence Ops", *Spaceflight Now*, January 14, 2009, available at: www.spaceflightnow.com.
36. M. Gruss, "Air Force Sent GSSAP Satellite to Check on Stalled MUOS-5", *SpaceNews*, August 18, 2016, available at: http://spacenews.com.
37. K. Pfrang and B. Weeden, "Russian Military and Intelligence Rendezvous and Proximity Operations", *Fact Sheet*, Secure World Foundation, August 2020.
38. This was the technique used by the Soviet Istrebitel Sputnik (IS) system. See K. Pfrang and B. Weeden, "Russian Co-Orbital Antisatellite Testing", *Fact Sheet*, Secure World Foundation, August 2020.

Warning time of such a close approach would likely be at least hours (for LEO) or days (for GEO), unless the attacking satellite was already in a very similar orbit to the target.

Direct Ascent ASAT

Direct ascent ASATs (DA-ASATs) use a ground, air, or sea-launched rocket to place a kinetic kill vehicle (KKV) on a ballistic trajectory up into space. After separation from the rocket, the KKV uses onboard guidance, navigation, and control systems to identify and track a targeted space object and fine-tune its trajectory to create a hypervelocity collision (direct hit), often at speeds in excess of 10 kilometers per second of relative velocity. The hit-to-kill (HTK) technique used by DA-ASATs is similar to how midcourse missile defense interceptors target nuclear warheads travelling through space, with the difference being the targeted nuclear warheads are on ballistic, instead of orbital, trajectories. Unlike a co-orbital ASAT, a DA-ASAT KKV itself does not have enough velocity to achieve orbit. Thus, when trying to anticipate the amount of space debris remaining in the long-term, one should distinguish the resulting fragments of the DA-ASAT KKV, unlikely to remain in orbit very long, from the fragments from the orbital object that was struck, which are likely to remain in space after the collision.

The Chinese direct-ascent ASAT program has its roots in several anti-ballistic and surface-to-air missile programs that emerged from the 1960s through the 1990s. Since then, China has demonstrated significant advances in HTK capability and engaged in large-scale modernization and development efforts for advanced rocket technology — tracking, targeting, and SSA capabilities — and launch infrastructure, both mobile and stationary. China may be developing as many as three direct-ascent ASAT systems, although it is unclear whether all three are intended to be operational or whether their primary mission is counterspace or midcourse missile defense.

The main Chinese DA-ASAT capability leverages a ground-launched missile labeled the SC-19 by Western intelligence. The SC-19 is likely a variant of the Chinese DF-21C road-mobile medium-range ballistic missile but may also incorporate some elements of the HQ-19 midcourse missile defense system.[39] The SC-19 was first quietly tested in 2005 and 2006 from the Xichang Satellite Launch Center in Sichuan with what appears to be

39. R. Fisher, *China's Military Modernization: Building for Regional and Global Reach*, Standford, CA: Standford University Press, 2008, pp. 2, 131; S. O'Connor, "PLA Ballistic Missiles", *Air Power Australia Technical Reports*, Air Power Australia, January 27, 2014, available at: www.ausairpower.net.

rocket tests or planned misses.[40] A more spectacular tested occurred in 2007 when it was used to destroy an older Chinese weather satellite, the FengYun 1C, at an altitude of 863 kilometers and created nearly 3,000 pieces of long-lived orbital debris. Testing then moved to the Korla Missile Test Complex, with additional launches in January 2010, January 2013, and July 2014. At least two of these tests (2010 and 2013) included intercepts of ground-launched ballistic missile targets that did not produce orbital debris.[41]

Additional tests have fueled speculation about a new ground-launched DA-ASAT system. Three more tests were done in October 2015, July 2017, and February 2018 from either Korla or the Jiuquan Satellite Launch Center and all three were characterized by anonymous U.S. officials as being of a new system labeled the DN-3 by Western intelligence.[42] However, the publicly-available information is inconclusive to prove whether these tests were of the same system as the SC-19, a new version with upgraded capabilities, or a midcourse missile defense system that has latent ASAT capabilities.

An unusual launch from the Xichang Satellite Launch Center in May 2013 indicated that there may be a third Chinese DA-ASAT capability in development. On May 13, 2013, China launched a rocket from Xichang, which the Chinese Academy of Sciences stated was a high-altitude scientific research mission. A U.S. military official stated that "the launch appeared to be on a ballistic trajectory nearly to [GEO]. We tracked several objects during the flight…and no objects associated with this launch remain in space," but unofficial U.S. government sources say it was actually a test of a new ballistic missile related to China's ASAT program.[43]

Although there is no public proof that the launch in May 2013 was indeed a test of a new ASAT system, the publicly-available evidence is more in line with a direct ascent ASAT test than a scientific experiment.[44] The details of the launch were different from those of either a standard satellite launch to GEO or the launch of a sounding rocket such as the high altitude reached, nearly 36,000 kilometers, and a flight trajectory beyond the capability of the previous SC-19. Google Earth satellite imagery of Xichang indicates that there were no known Chinese space launch vehicles on the

40. M. R. Gordon and D. S. Cloud, "U.S. Knew of China's Missile Test, but Kept Silent", *The New York Times*, April 23, 2007.
41. B. Weeden, "Chinese Direct Ascent Anti-satellite Testing" *Fact Sheet,* Secure World Foundation, August 2020.
42. B. Gertz, "China Carries Out Flight Test of Anti-Satellite Missile", *The Washington Free Beacon*, August 2, 2017, available at: http://freebeacon.com.
43. B. Weeden, "Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space", *The Space Review*, March 17, 2014, available at: www.thespacereview.com.
44. *Ibid*.

launch pad that matched the description of the rocket given in the Chinese media. However, a commercial satellite image taken on April 3, 2013, did show what appears to be a transporter-erector-launcher (TEL), usually associated with mobile ballistic missiles, on a mobile launch pad constructed at Xichang between November 2006 and April 2012.[45] An analysis of the launch trajectory indicates that a re-entry over the Indian Ocean is consistent with a ballistic trajectory that has an apogee around 30,000 kilometers.

Recent reporting suggests that at least one of the Chinese DA-ASAT systems, likely the SC-19 or its follow-on, has achieved operational status. In December 2018, the National Air and Space Intelligence Center (NASIC) released a public counterspace assessment of foreign space and counterspace capabilities that stated, "China has military units that have begun training with anti-satellite missiles."[46] In his statement for the record before the United States Senate on January 29, 2019, Director of National Intelligence Daniel Coats stated that China "has an operational ground-based ASAT missile intended to target low-Earth-orbit satellites."[47] Taken together, these statements suggest that China has operationally deployed DA-ASAT systems to at least some units and has developed operational training for their use, although there has not been independent confirmation of this via open sources.

45. *Ibid.*

46. National Air and Space Intelligence Center, "Competing in Space", December 2018, available at: https://media.defense.gov.

47. D. Coats, "Worldwide Threat Assessment of the United States Intelligence Community", *Statement for the Record*, Senate Select Committee on National Intelligence, January 29, 2019, available at: www.intelligence.senate.gov.

Table 2 – History of Chinese DA-ASAT Tests

Date	ASAT System	Site	Target	Apogee	Notes
July 7, 2005	SC-19	Xichang	None known	??	Likely rocket test
Feb. 6, 2006	SC-19	Xichang	Unknown satellite	??	Likely near-miss of orbital target
Jan. 11, 2007	SC-19	Xichang	FY-1C satellite	865 km	Destruction of orbital target
Jan. 11, 2010	SC-19	Korla	CSS-X-11 ballistic missile launched from Jiuquan	250 km	Destruction of target
Jan. 20, 2013	Possibly SC-19	Korla	Unknown ballistic missile launched from Jiuquan	Suborbital	Destruction of target
May 13, 2013	Possibly DN-2	Xichang	None known	~30,000 km	Likely rocket test
July 23, 2014	Possibly DN-2, (possibly SC-19)	Korla? (Jiuquan?)	Likely ballistic missile launched from Jiuquan	Suborbital	Likely intercept test
Oct. 30, 2015	Possibly DN-3	Korla	None known, possible ballistic missile	Suborbital	Likely rocket test
July 23, 2017	DN-3	Jiuquan?	Likely ballistic missile	Suborbital, malfunctioned	Likely intercept test
Feb. 5, 2018	DN-3	Korla	CSS-5 ballistic missile	Suborbital	Likely intercept test

China's development, testing, and potential deployment of DA-ASAT capabilities are similar to previous and current programs by both the United States and Russia. The United States tested the first air-launched DA-ASAT, a modified version of the High Virgo air launched ballistic missile, in

September 1959.[48] By the early 1960s, the United States had an operational DA-ASAT on Kwajalein Atoll in the Pacific Ocean, albeit with a 1.4 megaton nuclear warhead because the technology of the time did not allow for reliable HTK.[49] In the late 1970s, the United States began a program to develop an air-launched DA-ASAT that was carried by an F-15 fighter jet, which included an intercept test that used a KKV to destroy NASA's Solwind satellite in 1985.[50] In February 2008, the United States used as modified SM-3 midcourse missile defense interceptor to destroy the USA 193 spy satellite that was feared to contain toxic frozen fuel that could pose a threat on atmospheric re-entry.[51]

Russia also has a history of developing and testing DA-ASATs. The Soviet Union explored several different types of DA-ASAT capabilities during the Cold War and the exoatmospheric interceptors for the A-135 missile defense system around Moscow likely had a DA-ASAT capability.[52] Since early 2000s, Russia appears to have resurrected at least a few of the Cold War era DA-ASAT programs, including the air-launched Kontakt missile and the Nudol ground-mobile missile.[53] The Nudol has been tested at least ten times since 2014, although the first two were failures and it is unknown if any of the later tests were planned to be intercepts. To date, the Nudol has not been used to successfully destroy a space object.

The main concern generated by the current Chinese DA-ASAT program is that these weapons could be used to destroy important national security satellites in LEO, perhaps up to an altitude of 1000 kilometers. This threat bubble would include many critical U.S. intelligence, surveillance, and reconnaissance (ISR) and military weather satellites as well as similar satellites operated by other countries. China would have to wait for such satellites to overfly an area where one of the DA-ASAT systems is deployed, but most LEO satellites would do so daily or every few days. Once launched,

48. A. Parsch, "WS-199", *Designation-Systems.Net*, November 1, 2005, available at: www.designation-systems.net.

49. B. Weeden, "Through a Glass, Darkly Chinese, American, and Russian Anti-satellite Testing in Space", *The Space Review*, March 17, 2014, available at: https://swfound.org.

50. The four other tests include: a successful missile test without the MHV on January 21, 1984; a failed missile test directing MHV at a star on November 13, 1984; and two successful flight tests directing MHV at a star on August 22, 1986 and September 29, 1986. See G. Karambelas and S. Grahn, "The F-15 ASAT Story", *Sven's Space Place*, available at: www.svengrahn.pp.se; R. Puffer, "The Death of a Satellite", Edwards, CA: Air Force Flight Test Center History Office, archived from web in 2003, available at: https://web.archive.org.

51. "Navy Missile Hits Dying Spy Satellite, Says Pentagon", *CNN*, February 21, 2008, available at: http://www.cnn.com.

52. R. K. Kommel and B. Weeden, "Russian Direct Ascent ASAT Testing", *Fact Sheet*, Secure World Foundation, August 2020.

53. *Ibid.*

the target would only have an estimated 5 to 15 minutes warning time before impact, making it very difficult to maneuver to avoid destruction.

While China has only conducted the one DA-ASAT test to orbits beyond LEO, it is theoretically possible to use such capabilities to target satellites in orbits all the way out GEO at more than 36,000 kilometers. GEO includes additional critical ISR satellites as well as satellites use for missile warning and military communications. However, DA-ASAT attacks against satellites at these altitudes would have the disadvantage of flight times of at least several hours, giving plenty of time for detection and countermeasures.

Electronic Warfare

Electronic warfare (EW) is defined as "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[54] In the context of counterspace capabilities, the scope of EW is narrowed to refer specifically to intentional interference with an adversary's radiofrequency (RF) transmissions to or from a satellite. This intentional interference is often referred to as "jamming". In some cases, the interfering signal may attempt to pose as the real signal to end users, which is referred to as "spoofing".

In the case of satellite signals, jamming is often characterized as being either uplink or downlink. Uplink jamming occurs when an outside RF signal is aimed at the satellite directly. Most communication satellites serve as a relay node that rebroadcast signals directed at it (uplinked) from the ground. The uplink interference signal can originate anywhere within the ground footprint of the receive antenna and overwhelms the intended signal such that the signal re-transmitted by the satellite and received by the users on the ground consists of a garbled mix of the intended signal and the jamming signal. The impact may be widespread since all users within the satellite's broadcast footprint are affected. Downlink, or terrestrial, jamming targets the ground user of satellite services by broadcasting a RF signal that overwhelms the intended satellite signal for users in a specific area on the ground. In downlink jamming, the satellite itself suffers no interference, nor would users outside the range of the jammer.

Evidence suggest China is developing a broad range of EW capabilities for counterspace applications. One main area is jamming or interference with signals from global navigation satellite systems (GNSS), such as the Global Positioning System (GPS) operated by the U.S. military and the European Galileo system operated by the European Space Agency. These

54. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington DC: The Joint Staff, June 2020, p. 71.

systems work by broadcasting RF timing signals from a constellation of satellites orbiting at an altitude of roughly 20,000 kilometers. Receiving at least four of these signals allows an end user device to calculate its position and altitude to a high degree of precision. Most of these systems broadcast separate civil signals, which are intended for general use and usually lack any encryption or spoofing protection, and military signals that have encryption and other protections against jamming and spoofing.

GNSS jamming and interference, particularly of the civil signals broadcast by GPS, is a well-known technology and jammers are widely proliferated throughout the globe. China is proficient in GPS jamming capabilities, having developed both fixed and mobile terrestrial systems. The known systems are downlink jammers, which affect GPS receivers within a local area near the source of the jamming. There is no known system that targets uplink jamming of the GPS satellites themselves, nor is there public evidence of China testing space-based GPS jammers.

Recent incidents highlight the extent and sophistication of Chinese GNSS jamming. In November 2019, a report detailed multiple incidents of GNSS jamming and spoofing near the Chinese port of Shanghai.[55] Analysts from the Center for Advanced Defense Studies determined that jamming and spoofing of the GNSS signals used by the automatic identification system (AIS) to track commercial shipping began in the summer of 2018. The attacks culminated in July 2019 with spoofed locations for over three hundred ships in Shanghai or the Huangpu River on a single day. The effect of the spoofing was also unique: the position of the ships was jumping every few minutes in a ring pattern that showed as large circles over weeks. Additional analysis showed that the spoofing was affecting fitness tracks as well, suggesting it was impacting all GPS receivers in the area.

Two other major areas where EW has counterspace applications are interfering with satellite communications signals and imagery satellites using synthetic aperture radar (SAR) for ISR collection. While public evidence of Chinese capabilities to disrupt satellite communications and SAR is scarce, the January 2019 DIA space and counterspace report states that China is developing jammers to target satellite communications and SAR over a range of frequency bands, including those used by the U.S. military, citing Chinese scientific papers describing the status of research and potential operational techniques.[56] There is also the potential for China to develop space-based EW capabilities, likely paired with RPO capabilities

55. M. Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai", *MIT Technology Review*, November 15, 2019, available at: www.technologyreview.com.
56. "Challenges to Security in Space", Defense Intelligence Agency, Report, Washington, D.C., January 2019, p. 20.

to jam or interfere with satellites from closer range than terrestrial-based EW weapons. While there is some evidence that Russia is developing these technologies,[57] to date we do not have evidence that China is doing so.

It is unknown if China possesses the ability to interfere with military GNSS signals. To date, all of the publicly known incidents of Chinese GNSS jamming and interference have been against the civil GPS signals. However, the legacy military GPS signal overlaps the same frequency as the civil GPS signal, meaning that jamming or spoofing the civil signal alone could create challenges for military users.[58] This problem is being addressed with the new military GPS signal, known as M-Code, and a corresponding new generation of military GNSS receivers that use M-Code[59] and could also be addressed by using protected signals from other GNSS such as the Galileo PRS.[60]

Looking ahead, we can expect China – and other countries – to improve and expand their ability to interfere with satellite signals, particularly on GNSS. The technology is robust and advancing faster than the protections, given that most satellites last on orbit for several years or more and are often backwards compatible with existing user bases. Protecting GNSS is even more of a challenge because of the massive installed base and the lack of any real anti-jam or anti-spoofing protections on the civil signals.

Directed Energy

Directed Energy weapons (DEW) refers to a class of potential weapons technologies that harness concentrated beams of electromagnetic waves or subatomic particles. The three main types of DEWs are lasers, particle beams and RF energy (also known as high-power microwave) weapons. Of these, laser systems are the most developed and prominent of the DEW counterspace threats.

Laser systems for counterspace applications could be either ground-based or space-based. Ground-based systems require much higher power to penetrate the atmosphere but have few restrictions on size, type and consumptions of chemicals or electrical power. Space-based systems, on the other hand require less power to have similar effects but are typically carried on platforms that are severely restricted in size and power availability. For example, ground-based chemical lasers can generate high power but would

57. B. Hendrickx, "Russia Gears Up for Electronic Warfare in Space", *The Space Review*, November 2, 2020, available at: www.thespacereview.com.
58. M. Jones, "New Military Code about to Board 700+ Platforms", *GPS World*, April 9, 2019, available at: www.gpsworld.com.
59. *Ibid.*
60. "Delay Continues for Effort to Add Galileo Signal to U.S. Military Receivers", *Inside GNSS*, November 16, 2017, available at: https://insidegnss.com.

be difficult to implement in space due to their size and the disturbance torques that may be generated by exhaust. Solid state and fiber lasers would be more appropriate for space basing but require large inputs of electrical energy.

Lasers can be used for counterspace applications in a few different ways. The first is to dazzle or temporarily interfere with the optics of a satellite. This can happen when the light from a laser enters the optics of a satellite sensor and overwhelms the underlying circuitry used to sense photons, causing the resulting imagery to be washed out or having bright spots. Relatively low power (10 or more Watts) lasers could be used for dazzling, although there are countermeasures such as tripping a physical shutter or looking off-axis from the laser site. In addition, although the dazzling effect is usually temporary, it can be difficult to judge the level at which a dazzler could permanently damage the sensor, particularly without detailed knowledge of its inner workings. Lasers of more than 100 or so Watts are likely to cause permanent damage to optics. Very high power ground-based lasers (thousand to millions of Watts) could be used to physically damage the satellite bus itself, such as solar panels or batteries. Whether or not the laser operates in pulse or continuous wave mode also affects its ability to inflict damage.

China has been actively pursuing DEW for counterspace and other applications since the 1960s, and there are significant scientific and technical discussions of research and possible future military applications as part of the Project 640 anti-ballistic missile program.[61] However, exactly how advanced Chinese DEW counterspace weapons are is unknown and there is very little public evidence of their deployment or use.

Open source research suggests there are three main sites supporting China's DEW work.[62] The first two are the Center for Atmospheric Optics at the Anhui Institute for Optics and Fine Mechanics in Hefei, Anhui Province, and the Chinese Academy of Engineering Physics campus in Mianyang, Sichuan Province. Both facilities have similar large, rectangular buildings with retractable roofs that suggest facilities where DEW aimed at satellites could have been developed. The retractable roofs allow the lasers to be aimed at satellites passing overhead. The third site is located near the Korla Missile Test facility in Xinjiang Province and features camouflaged buildings and security fences that strongly suggest it is operated by the military. In March 2019, a retired Indian Air Force officer published an article showing

61. *China's Progress with Directed Energy Weapons*, U.S.-China Economic and Security Review Commission, Testimony by Richard D. Fisher, February 23, 2017.
62. B. Weeden and V. Samson, *Global Counterspace Capabilities: An Open Source Assessment*, *op. cit.*

commercial satellite imagery of the DEW facility near Korla and the four buildings suspected of housing laser weapons.[63]

There are only a few publicly known instances of China used DEW against satellites. In 2006, a news report cited anonymous U.S. defense officials who claimed that China had used ground-based lasers to "dazzle" or blind U.S. optical surveillance satellites on multiple occasions.[64] Subsequent reporting suggested that the satellites may have been merely illuminated by the lasers and senior U.S. officials at the time stated that no U.S. satellites were materially damaged. In December 2013, an article in a Chinese scientific journal stated that a successful laser blinding test had been carried out in 2005 against a LEO satellite at 600 km altitude.[65] China also operates several satellite laser ranging sites that are part of the International Laser Ranging Service (ILRS), which could theoretically be used to dazzle satellites, but to date there's no public information that has occurred.[66]

Chinese capabilities for using DEW for counterspace applications are likely to improve in the coming years. While laser weapons technology has lagged many of the public proclamations over the last few decades, R&D investment has continued and is likely showing some payoff. The most likely capability that will be deployed is the ability to use ground-based DEWs to dazzle electro-optical imagery satellites and prevent them from imaging sensitive ground installations near the DEW site. These capabilities may also result in some unintentional or intentional permanent damage to the satellites' optics but are unlikely to reach the point where broader physical damage to a satellite is possible from the ground in the next few years. China may also be able to develop the ability to mount DEW onboard satellites, which could be combined with RPO capabilities to cause physical damage or interfere with the electronics of a target satellites from close range. However, this likely requires significant advances in on-board power generation technologies to be feasible, particularly if intended for a small satellite platform. That said, co-orbital dazzling from close range is probably feasible given the current state of light detection and ranging (LIDAR) technology.

63. V. Bhat, "These Futuristic Chinese Space Denial Weapons Can Disable or Destroy Opposing Satellites", *The Print*, March 23, 2019, available at: https://theprint.in.
64. G. Kessler, "Bachman's Claim that China 'Blinded' U.S. Satellites", *The Washington Post*, October 4, 2011.
65. G. Min-hui *et al.*, "Development of Space Based Laser Weapons", *Chinese Optics*, December 2013, available at: www.chineseoptics.net.cn.
66. Satellite laser ranging is used for precise measurement of orbital trajectories. See Y. Butt, "Effect of Chinese Laser Ranging on Imaging Satellites", *Science and Global Security*, Vol. 17, No. 1, June 8, 2009, pp. 20-35.

Cyber

Cyber attacks against space capabilities are similar to cyber attacks against non-space systems. They often involve attempts to feed user-provided information to a system that causes software to perform in unexpected ways, commonly known as ”bugs”. In some cases, bugs can be exploited to crash systems, run unauthorized code, and/or gain unauthorized access. Other common cyber attacks exploit the lack of or faults in authentication of users and commands. The more software features or components a system has, and the more types and channels of data it processes, the higher the attack surface of potential vulnerabilities that an attacker can exploit. There is also an unclear distinction between cyber attacks and electronic warfare, with some arguing for a merger of the two fields.[67]

Cyber attacks pose a significant threat to space systems.[68] Modern satellites are increasingly “computers in space” that leverage similar architectures, components, and software to computers in general. However, unlike desktop computers or mobile devices, the vast majority of satellites are not directly connected to the Internet. Instead, they are usually connected via radio frequency or laser links to dedicated or leased ground stations. Those ground stations in turn are linked to facilities where operators use standard computers to send commands to the satellites or receive data from the satellites. This means that a cyber attack against the ground station, command and control facility, or end user device could be just as successful, and easier to accomplish, as a cyber attack directly against the satellite.

There have been very few publicly acknowledged cyber attacks against satellite systems and even fewer that have been positively attributed to China. Space-related cyber attacks linked to China include a set of attacks against command and control links for NASA satellites between 2007 through 2009, including at least one where the attackers achieved “all steps required to send commands [to the satellite] but did not.”[69] The U.S. cybersecurity firm Symantec reported in 2018 on a wide-ranging cyber espionage campaign by a group named Thrip, likely based in China, that included attacks targeting computers at a commercial operator running

67. E. Chabrow, “Aligning Electronic and Cyber Warfare”, *Gov Info Security*, July 10, 2012, available at: www.govinfosecurity.com.
68. “Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems”, Washington, D.C.: The White House, September 4, 2020.
69. U.S. Economic and Security Review Commission, “2011 Report to Congress of the U.S.-China Economic and Security Review Commission”, November 2011, p. 216.

software that monitors and controls communications satellites.[70] Cyber attacks have also happened against the computer systems used to distribute satellite data. In late 2014, attackers breached NOAA's computer network, including systems used to manage and disseminate satellite weather data and products for the National Environmental Satellite, Data, and Information Service (NESDIS) and the National Earth System Prediction Capability (ESPC).[71] While the U.S. government did not publicly attribute the attack, Representative Frank Wolf declared that "NOAA told me it was a hack and it was China."[72]

China's capabilities for conducting cyber attacks are likely to increase in the future years. The space sector is generally behind where other major sectors (manufacturing, energy, transportation, etc.) are in recognizing the threat of cyber attacks and instituting mitigation measures across the entirety of the sector. At the same time, offensive cyber capabilities tend to be developed faster than defensive mitigation steps can be implemented. This is particularly true in space, where most satellites tend to be in development for years and are operational on orbit for years to decades, leaving a large installed base of legacy systems. Satellite operators are also relatively risk averse when it comes to pushing software patches or upgrades because of the challenges of recovering from a system failure or anomaly.

Space Situational Awareness

SSA is the ability to accurately characterize the space environment and activities in space. Civil SSA combines positional information on the trajectory of objects in orbit (mainly using optical telescopes and radars) with information on space weather. Military SSA, also known as Space Domain Awareness (SDA), also includes characterizing objects in space, their capabilities and limitations, attempting to model or predict their behaviors, and identifying potential threats.

SSA is traditionally done with ground-based radars and telescopes. Radar consists of at least one transmitter and receiver that emit radio waves at a specific frequency that reflect off the target. Optical telescopes collect light or other electromagnetic (EM) radiation emitted or reflected by an object and focused into an image using lenses, mirrors, or a combination of the two. The reflected radio waves or light can be measured to calculate where an object in space is relative to the sensor. Multiple measurements

70. Security Response Attack Investigation Team, "Thrip: Espionage Group Hits Satellite, Telcoms, and Defense Companies", *Symantec*, June 19, 2018, available at: www.symantec.com.
71. M. Pat Flaherty *et al.*, "Chinese Hack U.S. Weather Systems, Satellite Network", *The Washington Post*, November 12, 2014.
72. *Ibid.*; T. Cama, "Report: Chinese Hacked U.S. Weather Systems", *The Hill*, November 12, 2014.

over time can be used to estimate the object's orbital trajectory. When combined with sophisticated models of the Earth's gravitational field, atmospheric density, and space weather, it is possible to propagate orbital trajectories forward into the future and predict potential close approaches, overflight locations, and other applications. Other types of sensors, including sensors that detect radio frequency (RF) or other types of signals from satellites, lasers that measure the distance or range to a satellite very accurately, and infrared sensors that detect heat, can be used to help refine orbits or characterize a space object.

China's main optical SSA capabilities are operated by the Purple Mountain Observatory (PMO), which operates multiple telescopes in seven separate locations in China that can track satellites throughout all orbital regimes.[73] PMO originated from civilian and scientific research on astronomy and maintains a strong scientific focus. Since the early 2000s, PMO has increasingly been involved in tracking human-generated space objects and orbital debris and is China's main contributor to the Inter-Agency Space Debris Coordination Committee (IADC) that does research on orbital debris.[74]

Few details are known about China's radar SSA capabilities as they are primarily operated by the PLA. The PLA operates at least four large phased-array radars (LPARs) that likely have a primary mission of ballistic missile warning but could also support an SSA mission. The existing radars are located near Huanan (46.53N, 130.76E), Yiyuan (36.02N, 118.09E), Hangzhou (30.29N, 119.13E), and Korla (41.64N, 86.24E).[75] The radars are approximately 30 meters in diameter and likely have a coverage arc of 90 to 120 degrees, similar to a U.S. Ballistic Missile Early Warning System (BMEWS) radar.[76] The Korla radar can be rotated and is likely used to support the ballistic missile and ASAT testing done at Korla.

In June 2015, China launched the Space Debris Monitoring and Application Center to collate SSA data from various sensors and help protect Chinese satellites from on-orbit collisions. The Space Debris Monitoring and Application Center, part of the China National Space Administration, is responsible for tracking orbital debris, analyzing hazards, developing prevention and disposal plans, setting up a database and communicating

73. "About Purple Mountain Observatory (PMO)", *Purple Mountain Observatory*, available at: http://english.pmo.cas.cn.
74. C. Choi, "China Says Work Under Way to Mitigate Space Junk", *Space.com*, September 3, 2007, available at: www.space.com.
75. A. Tate, "China Integrates Long-range Surveillance Capabilities", *IHS Jane's*, 2017, available at: www.janes.com.
76. *Ibid.*

with other nations and international organizations.[77] Officials stated that the Center would provide early warnings of close approaches and possible collisions to Chinese satellite operators.

China also maintains a global network of satellite tracking stations, which may have some SSA capabilities. China maintains a fleet of Yuanwang ships that are primarily used to support Chinese space launches.[78] The ships will deploy to areas around the world where they can augment China's ground-based satellite tracking, telemetry, and control (TT&C) located in its territory. In addition, China has signed agreements to host ground-based tracking stations in Karachi, Pakistan; Swakopmund, Namibia, Malindi, Kenya; Dongara, Australia; Santiago, Chile; Alcantara, Brazil; Neuquén, Argentina; and Kiruna, Sweden.[79] All of these TT&C capabilities are coordinated through the Xi'an Satellite Measurement and Control Center. Typically, TT&C facilities use antennas to detect signals from active satellites and broadcast commands to them or receive transmissions from them, which would not be able to track orbital debris or satellites broadcasting on different frequencies. These facilities may include telescopes or other SSA sensors that could do such tracking, and their spread has prompted concerns about the PLA using them for military operations or espionage.[80] However, to date there is no evidence that the international TT&C sites operated by China are fundamentally different from those operated by other countries.

In addition to its national effort, China has also engaged in international cooperation efforts on SSA through the Asia-Pacific Space Cooperation Organization (APSCO). APSCO is a China-led intergovernmental organizational for space cooperation that includes Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey as members and Mexico as an observer.[81] In 2012, APSCO kicked off the Asia-Pacific Ground-Based Space Object Observation System (APOSOS) Phase 1 project to integrate data from three telescopes in Pakistan, Peru, and Iran with a Data Centre in Beijing.[82] In April 2019, APSCO kicked off the Asia-Pacific Space Science Observatories (APSSO) Project that expanded the scope of APOSOS and included plans for a future Space Debris Observation

77. N. Chen, "Agency Set to Track, Deal with Space Junk", *Chinese Academy of Sciences*, June 10, 2015, available at: http://english.cas.cn.
78. C. Guoling and Z. Weirong, "China Advances Maritime Space Monitoring and Control Capability", *Ministry of Defense of the People's Republic of China*, June 23, 2017, available at: http://eng.mod.gov.cn.
79. E. Kania, "China's Strategic Situational Awareness Capabilities", *Issue Briefs*, Center for Strategic and International Studies, Spring 2019.
80. V. Robert Lee, "China Builds Space-Monitoring Base in Argentina", *The Diplomat*, May 24, 2016.
81. "About APSCO", *Asia-Pacific Space Cooperation Organization*, accessed on February 18, 2020, available at: www.apsco.int.
82. "Ground-Based Space Object Observation Network", *Asia-Pacific Space Cooperation Organization*, accessed on February 18, 2020, available at: www.apsco.int.

and Data Application Center (SDOAC).[83] While some publications have described APOSOS as being fully capable of providing global GEO coverage,[84] the publications from ASPCO suggest the project is still nascent and has only limited capabilities.

China's work on space weather is conducted through the National Space Weather Monitoring and Warning Centre, which was established by the Central Planning Committee in 2002 and is part of the China Meteorological Administration.[85] The Center provides daily space weather forecasts and warnings of severe space weather based mainly off sensors and payloads carried by the Feng Yung series of meteorological satellites in LEO and GEO. China is a member of the Asia-Oceania Space Weather Alliance and the International Space Environmental Service (ISES) where it shares space weather data with fourteen other countries.[86]

China, like many other countries, is likely to improve its SSA capabilities in the coming years. China recognizes that the ability to monitor activities in space is critical for protecting its own satellites from environmental and hostile threats as well as targeting potential adversary satellites for attacks. This motivation will increase as China continues to develop its own satellite constellations to support national security, science, and socioeconomic objectives. In particular, the forthcoming launch of the Chinese Space Station and increased human spaceflight activities are likely to spur a significant increase in Chinese focus on SSA.

83. "NewsAPSCO", *Asia-Pacific Space Cooperation Organization*, April 2019, available at: www.apsco.int.
84. "Challenges to Security in Space", Defense Intelligence Agency, Report, Washington, D.C., January 2019.
85. "Space Weather Products", *National Center for Space Weather*, accessed on February 18, 2020, available at: www.nsmc.org.cn.
86. "Members", *International Space Environment Service*, accessed on February 18, 2020, available at: www.spaceweather.org.

Implications for Europe and Transatlantic security

While Russian development of counterspace capabilities currently poses the most significant threat to European space capabilities, Chinese counterspace capabilities could present a potential future threat in various ways. In the current geopolitical climate, it is unlikely that Europe would find itself in a direct, major military confrontation with China. While China may have a long-term desire to wield global military strength, for the foreseeable future it is focused on exerting more military strength on its borders and regionally. The vast majority of China's military development, and in particular military space capabilities, are aimed at being able to push potential adversaries away from its borders and potentially conduct military operations in neighboring areas such as the Taiwan Straits, South China Sea, and its border with India.

That said, there is the possibility that Europe could be pulled into a U.S.-China armed conflict that is taking place in East Asia. The United States has existing defense agreements and alliances with several countries in the region, including Japan, Taiwan, South Korea, the Philippines, and Australia, and strong domestic support to defend its allies and national interests against Chinese aggression. The United States may also invoke Article 5 of the North Atlantic Treaty and call for European members of NATO to come to its collective defense in an armed conflict with China.[87]

For its part, the United States sees allied space capabilities as an important element of increasing the resilience of its own space systems. The United States would likely be very interested in leveraging European capabilities such as Galileo, space-based ISR, and ground-based SSA capabilities in an armed conflict with China to augment its own capabilities and potentially replace capabilities destroyed by Chinese counterspace attacks. Even if the United States was not directly using European space systems, China may presume it is using them, or will use them, and may consider them to be valid military targets. In the near-term, this suggests that the United States should discuss with its European allies what

87. While Article 6 of the NATO Treaty places geographic restrictions on the invoking of Article 5, it may still be the case that the United States puts political pressure on NATO countries to come to its defense in a conflict with China. See B. C. Grady, "Article 5 of the North Atlantic Treaty: Past, Present, and Uncertain Future", Vol. 31, No. 1, *Ga. J. Int'l & Comp. L.*, 2002.

capabilities may be available and how best to leverage cross-investments to augment each other's capabilities.

Even if Europe was not directly involved in a U.S.-China armed conflict, the conflict may have severe repercussions for Europe. Large numbers of Chinese or American kinetic attacks against satellites would create huge amounts of orbital debris, portions of which may remain on orbit for decades and pose a significant collision risk to European satellites. Widespread jamming or interference with GNSS, even limited to the Asia-Pacific region, would likely have a negative impact on global transportation systems. Destruction of civil dual use U.S. and Chinese remote sensing satellites may impact global meteorological and climate modeling and weather forecasting.

The more likely scenario is that Europe will have to deal with Chinese counterspace capabilities being used in a "grey zone" conflict that is outside actual armed conflict[88] or in continued peacetime competition.[89] The re-emergence of Great Power Conflict, as defined by the 2018 National Defense Strategy, likely means an increase in geopolitical tensions and competition between the United States and China in the Asia-Pacific region and perhaps beyond.[90] Offensive counterspace capabilities of a temporary nature, such as jamming or dazzling, may be used for research and development, strategic signaling, operational testing, annoyance tactics, or in support of proxy conflicts.

One area where European interests may be impacted by China's efforts to expand its influence is in the Indian Ocean. China has expanded its engagements in the Indian Ocean to include counterpiracy naval patrols, investment in strategic ports, and increased economic and security partnerships with countries in the region.[91] This expanded influence could impact Europe if China chose to exert influence over key international trade routes that support European markets, but the extent of China's desire and ability to do this is still uncertain.

The most important step for Europe in preparing to deal with these possibilities is to solidify European understanding of the situation. Historically, many European countries have tried to distance themselves

88. F. Hoffman, "Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges", *PRISM*, Vol. 7, No. 4, National Defense University, November 8, 2018.
89. The potential for this was highlighted by the European Commission in "EU-China: A Strategic Outlook", *Joint Communication to the European Parliament, the European Council, and the Council*, March 12, 2019.
90. Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America", January 2018. Whether or not Great Power Conflict exists, it is now the main driver for U.S. national security thinking and enjoys solid bipartisan support.
91. J. T. White, "China's Indian Ocean Ambitions: Investment, Influence, and Military Advantage", Washington, D.C.: The Brookings Institution, June 2020.

from national security and defense aspects of space activities, and some have explicitly defined peaceful uses of outer space as "non-military". Those countries are now in the minority for what is becoming a global militarization of space and proliferation of counterspace capabilities. This proliferation and potential use of counterspace capabilities in future conflicts could have significant implications for Europe, regardless of whether or not Europe is a party to the conflict.

European institutions must also recognize the threat and work at multiple levels to put in place mitigation measures. At the national level, European countries must understand what their national interests are, how they might be affected, and what national capabilities they may be able to provide in the event of a conflict extending into outer space. At the supranational level, the European Union needs to examine its space security policies and positions to decide how to improve the resilience of space capabilities that are fundamental to the economy, society, and its security, and what its defense policies are in responding to attacks on European space systems and increasing the resilience of those systems now.

Europe also has a chance to play a leading role in multilateral discussions to help address some of the space security challenges. Notably, the lack of existing norms of behavior for space activities and the uncertainty of how existing international law applies to military space activities, both in peacetime and during armed conflict, are exacerbating the situation. If the space domain is "normalizing" as a domain of military activities, then it behooves us to apply some of the same governance mechanisms to military space activities as exist in the land, sea, and air domains. Doing so can help increase the stability of outer space and reduce the chances that military actions in space may increase tensions or escalate to conflict on Earth. In addition, European SSA capabilities can help monitor space activities, identify irresponsible or hostile actions, and contribute to verification mechanisms for future space arms control or other legally-binding measure designed to improve space security and stability.

French Institute
of International
Relations