Global Counterspace Capabilities: An Open Source Assessment

April 2019

Promoting Cooperative Solutions for Space Sustainability

EXECUTIVE SUMMARY

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth, but also more congestion and competition in space. From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. The growing use of, and reliance on, space for national security has also led more countries to look at developing their own counterspace capabilities that can be used to deceive, disrupt, deny, degrade, or destroy space systems.

The existence of counterspace capabilities is not new, but the circumstances surrounding them are. Today there are increased incentives for development, and potential use, of offensive counterspace capabilities. There are also greater potential consequences from their widespread use that could have global repercussions well beyond the military, as huge parts of the global economy and society are increasing reliant on space applications.

This report compiles and assesses publicly available information on the counterspace capabilities being developed by multiple countries across five categories: direct-ascent, co-orbital, electronic warfare, directed energy, and cyber. It assesses the current and near-term future capabilities for each country, along with their potential military utility. The evidence shows significant research and development of a broad range of kinetic (i.e. destructive) and non-kinetic counterspace capabilities in multiple countries. **However, only non-kinetic capabilities are actively being used in current military operations.** The following provides a more detailed summary of each country's capabilities.

China

The evidence strongly indicates that China has a sustained effort to develop a broad range of counterspace capabilities. China has conducted multiple tests of technologies for rendezvous and proximity operations (RPO) in both low earth orbit (LEO) and geosynchronous orbit (GEO) that could lead to a co-orbital ASAT capability. However, as of yet, the public evidence indicates they have not conducted an actual destructive co-orbital intercept of a target, and there is no proof that these RPO technologies are definitively being developed for counterspace use as opposed to intelligence gathering or other purposes.

China has at least one, and possibly as many as three, programs underway to develop direct ascent anti-satellite (DA-ASAT) capabilities, either as dedicated counterspace systems or as midcourse missile defense systems that could provide counterspace capabilities. China has engaged in multiple, progressive tests of these capabilities since 2005, indicating a serious and sustained organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and likely in the process of being operationally fielded on mobile launchers. Chinese DA-ASAT capability against deep space targets - both medium Earth Orbit (MEO) and GEO - is likely still in the experimental or development phase, and there is not sufficient evidence to conclude whether there is an intent to develop it as an operational capability in the future.

China is likely to be developing directed energy weapons (DEW) for counterspace use, although public details are scarce. There is strong evidence of dedicated research and development and reports of testing, but limited details on the operational status and maturity of any fielded capabilities.

Although official Chinese statements on space warfare and weapons have remained consistently aligned to the peaceful purposes of outer space, privately they have become more nuanced. China has recently designated space as a military domain, and military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance. China has recently re-organized its space and counterspace forces, as part of a larger military re-organization, and placed them in a new major force structure that also has control over electronic warfare and

cyber. That said, it is uncertain whether China would fully utilize its offensive counterspace capabilities in a future conflict or whether the goal is to use them as a deterrent against U.S. aggression. There is no public evidence of China actively using counterspace capabilities in current military operations.

Russia

There is strong evidence that Russia has embarked on a set of programs over the last decade to regain some of its Cold War-era counterspace capabilities. Since 2010, Russia has been testing technologies for RPO in both LEO and GEO that could lead to or support a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. The technologies could also be used for non-aggressive applications, and the on-orbit testing done to date does not conclusively prove they are for an ASAT program. Recent evidence suggests Russia at least some of the recent LEO RPO activities are part of a LEO space situational awareness (SSA) and inspection capability, and that SSA capability may support a separate co-orbital ASAT program.

Russia is almost certainly capable of some limited DA-ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to U.S. space assets. Core Russian direct-ascent ASAT capabilities are not yet operational, and those currently in development are not planned to have the capability to threaten targets beyond LEO. Russia appears highly motivated to continue development efforts even where military utility is questionable, due at least in part to bureaucratic pressures.

Russia places a high priority on integrating electronic warfare (EW) into military operations and has been investing heavily in modernizing this capability. Most of the upgrades have focused on multifunction tactical systems whose counterspace capability is limited to jamming of user terminals within tactical ranges. Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of unmanned aerial vehicles (UAVs), guided missiles, and precision guided munitions, but has no publicly known capability to interfere with the GPS satellites themselves using radiofrequency interference. The Russian Army fields several types of mobile EW systems, some of which can jam specific satellite communications user terminals within tactical ranges. Russia can likely jam communications satellites uplinks over a wide area from fixed ground stations facilities. Russia has operational experience in the use of counterspace EW capabilities from recent military campaigns.

Russia has a strong technological knowledge base in directed energy physics and is developing a number of military applications for laser systems in a variety of environments. Russia has revived, and continues to evolve, a legacy program whose goal is develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no indication that an operational capability has been yet achieved. Although not their intended purpose, Russian ground-based satellite laser ranging (SLR) facilities could be used to dazzle the sensors of optical imagery satellites. There is no indication that Russia is developing, or intending to develop, high power space-based laser weapons.

Russian military thinkers see modern warfare as a struggle over information dominance and net-centric operations that can often take place in domains without clear boundaries and contiguous operating areas. To meet the challenge posed by the space-aspect of modern warfare, Russia is pursuing lofty goals of incorporating EW capabilities throughout its military to both protect its own space-enabled capabilities and degrade or deny those capabilities to its adversary. In space, Russia is seeking to mitigate the superiority of U.S. space assets by fielding a number of ground-, air-, and space-based offensive capabilities. Russia has recently re-organized its military space forces into a new organization that combines space, air defense, and missile defense capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

The United States

The United States has conducted multiple tests of technologies for RPO in both LEO and GEO, along with tracking, targeting, and intercept technologies that could lead to a co-orbital ASAT capability. These tests and demonstrations were conducted for other non-offensive missions, such as missile defense, on-orbit inspections, and satellite servicing, and the United States does not have an acknowledged program to develop co-orbital capabilities. However, the United States possesses the technological capability to develop a co-orbital capability in a short period of time if it chooses to.

While the United States does not have an operational, acknowledged DA-ASAT capability, it does have operational midcourse missile defense interceptors that have been demonstrated in an ASAT role against low LEO satellites. The

United States has developed dedicated DA-ASATs in the past, both conventional and nuclear-tipped, and likely possesses the ability to do so in the near future should it choose so.

The United States has an operational EW counterspace system, the Counter Communications System (CCS), which can be deployed globally to provide uplink jamming capability against geostationary communications satellites. Through its Navigation Warfare program, the United States has the capability to jam global the civil signals of global navigation satellite services (GPS, GLONASS, Beidou) within a local area of operation to prevent their effective use by adversaries and has demonstrated doing so in several military exercises. The U.S. likely has the ability to jam military GNSS signals as well, although the effectiveness is difficult to assess based on publicly-available information. The effectiveness of U.S. measures to counter adversarial jamming and spoofing operations against military GPS signals is not known.

The United States has had established doctrine and policy on counterspace capabilities for several decades, although not always publicly expressed. Most U.S. presidential administrations since the 1960s have directed or authorized research and development of counterspace capabilities, and in some cases greenlit testing or operational deployment of counterspace systems. These capabilities have typically been limited in scope, and designed to counter a specific military threat, rather than be used as a broad coercive or deterrent threat. The U.S. military doctrine for space control includes defensive space control (DSC), offensive space control (OSC), and is supported by space situational awareness (SSA).

Since 2014, U.S. policymakers have placed increased focus on space security, and have increasingly talked publicly about preparing for a potential "war in space." In the last two years they have publicly declared space to be a warfighting domain, although this is likely not a change in internal policy. This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems. Most recently, there has been a renewed public debate about reorganizing U.S. military space capabilities into a separate branch of the military, which may also take on a stronger counterspace role. It is possible that the United States has also begun development of new offensive counterspace capabilities, although there is no publicly available policy or budget direction to do so. There are recent budget proposals to conduct research and development of space-based missile defense interceptors and DEW that could have latent counterspace capabilities. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

Iran

Iran has a nascent space program, building and launching small satellites that have limited capability. Technologically, it is unlikely Iran has the capacity to build on-orbit or direct-ascent anti-satellite capabilities, and little military motivations to do so at this point. Iran has demonstrated an EW capability to persistently interfere with commercial satellite signals, although the capability against military signals is difficult to ascertain.

North Korea

North Korea has no demonstrated capability to mount kinetic attacks on U.S. space assets: neither a direct ascent ASAT nor a co-orbital system. In its official statements, North Korea has never mentioned anti-satellite operations or intent, suggesting that there is no clear doctrine in Pyongyang's thinking at this point. North Korea does not appear motivated to develop dedicated counterspace assets, though certain capabilities in their ballistic missile program might be eventually evolved for such a purpose. It is unlikely that North Korea would use one of its few nuclear weapons as an electromagnetic weapon.

North Korea has demonstrated the capability to jam civilian GPS signals within a limited geographical area. Their capability against U.S. military GPS signals is not known. There has been no demonstrated ability of North Korea to interfere with satellite communications, although their technical capability remains unknown.

India

India has over five decades of experience with space capabilities, but most of that has been civil in focus. It is only in the past several years that India has started organizationally making way for its military to become active users and creators of its space capabilities. India's military has been developing an indigenous missile defense program that its supporters argue could provide a latent ASAT capability, should the need arise; this capability was tested in an ASAT capacity in March 2019 after a reportedly unsuccessful test in February 2019. However, given how much investment the Indian military is making in its satellite capacity, India's continued insistence that it is against the weaponization of space, and

the income that Indian rockets are making launching other countries' satellites, it is unclear whether they will move to actively create an official counterspace program and they may just stop at having demonstrated an ASAT capability.

Cyber Capabilities

Multiple countries possess cyber capabilities that could be used against space systems; however actual evidence of cyber attacks in the public domain are limited. The United States, Russia, China, North Korea, and Iran have all demonstrated the ability and willingness to engage in offensive cyber attacks against non-space targets. Additionally, a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors.

There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyber attacks capabilities of leading nation-states and other actors.

2019 Additions

The following are brief summaries of the major additions for the 2019 edition of this report, broken down by country, along with a page reference to their location in the text. Individual minor changes or the impact of changes on summaries and assessments have been integrated into the text.

China

- Clarified the naming conventions and activities of the SY-7, SJ-15, and CX-3 payloads involved in a RPO in 2013 and 2014. (pg. 1-1)
- Added Table 1-6 on the longitudinal history of SJ-17 in the GEO region. (pg. 1-6))
- Added discussion of the Tongxin Jishu Shiyan (TJS)-3 satellite and subsatellite that conducted RPO in the GEO region in late 2018 and early 2019. (pg. 1-6)
- Added new reporting on the likely operational status of the SC-19 DA-ASAT system. (pg. 1-13)
- Added new section on Chinese DEW capabilities and programs. (pg. 1-17 to 1-20)
- Updated section on Chinese policy, doctrine, and organization to include recent changes to their military space and counterspace organizations. (pg. 1-22)

Russia

- Expanded discussion of recent Russian RPO activities in LEO to include new research suggesting they are part of an SSA program known as Nivelir ("Dumpy level")/Project 14K167 and may be supporting a new co-orbital program known as Burevestnik ("Petrel")/Project 14K168, both of which may have begun in 2011. (pg. 2-5 to 2-6)
- Updated RPO activities of Luch satellite to include close approach of Athena-Fidus, a French-Italian military communications satellite, and other satellites in GEO. (pg. 2-7)
- Added evidence that Russia may be upgrading the Krona optical space-based surveillance system with laser dazzling or blinding capabilities. (pg. 2-20 to 2-21)
- Updated section on Russian policy, doctrine, and organization to include recent changes to their military space and counterspace organizations. (pg. 2-24)

The United States

- Added more details on the RPO activities of the Geosynchronous Space Situational Awareness Program (GSSAP) satellites in the GEO region, including close approaches to multiple foreign commercial satellites. (pg. 3-5)

- Added details on the RPO activities of the Mycroft and the ESPA Augmented Geostationary Laboratory Experiment (EAGLE) satellites in the GEO region. (pg. 3-5 to 3-6)
- Added Table 3-2 summarizing recent U.S. RPO activities in LEO and GEO. (pg. 3-6)
- Added detail about U.S. jamming of GPS signals during recent military exercises. (pg. 3-11 to 3-12)
- Added new section on American DEW capabilities and programs for counterspace. (pg. 3-12 to 3-15)
- Updated section on American policy, doctrine, and organization to include recent proposals to change to their military space and counterspace organizations. (pg. 3-17 to 3-18)

Iran

- Add info about January and February 2019 satellite launches (pg. 4-1 to 4-2)

North Korea

- Added reports about Sohae Satellite Launching System potentially resuming operations. (pg. 5-2)

India

- Added new details about exoatmospheric testing of the Prithvi Air Defence (PAD) and endoatmospheric testing of the Advanced Area Defense (AAD) missile defense system. (pg. 6-2)
- Added initial reports of India's March 2019 Mission Shakti ASAT test after a prior failure in February 2019 (pg. 6-2)

Cyber

- Added details about the Thrip cyber espionage campaign that included attacks targeted at space-related companies and software services. (pg. 7-4)

Added claims about U.S. offensive cyber attacks aimed at Iran's ballistic missile program. (pg. 7-8)

Edited by

Brian Weeden, PhD, Director of Program Planning bweeden@swfound.org

Victoria Samson, Washington Office Director vsamson@swfound.org

Full report available at www.swfound.org/counterspace