UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Palais des Nations
CH-1211 Geneva 10
Switzerland

Phone +41 (0)22 917 17 93
Fax +41 (0)22 917 0176
www.unidir.org • @unidir

Counterspace Capabilities

Prepared for the United Nations Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space by the United Nations Institute for Disarmament Research[*]

Geneva, 6–17 August 2018

This backgrounder outlines demonstrated counterspace capabilities of six countries: the Democratic People's Republic of Korea (DPRK), the Republic of India, the Islamic Republic of Iran, the People's Republic of China, the Russian Federation and the United States of America. While there are reports of other countries developing counterspace capabilities, there is as yet insufficient publicly available data to confirm any demonstrations in the space context. The United States, China and Russia have thus far demonstrated the most advanced counterspace capabilities. The DPRK, India and Iran are also enhancing their capabilities, facilitated by the decreasing costs and ease in acquiring key technologies, and could readily develop counterspace technology.

This backgrounder is based on publicly available sources. It has drawn upon the Secure World Foundation's report on counterspace capabilities, *Global Counterspace Capabilities: An Open Source Assessment* as well as the Center for Strategic and International Studies' report, *Space Threat Assessment 2018*. Additional sources are credited in the notes.

*****

Categories of Counterspace Technology

- **Kinetic Physical**: Technology intended to create permanent and irreversible destruction of a satellite or to ground support infrastructure through force of impact with an object or a warhead. Such technology includes direct-ascent anti-satellite (DA-ASAT) missiles and co-orbital systems. The co-orbital systems are satellites placed on similar orbits and can be directed to intercept or interfere by means of a close orbital rendezvous.
- **Non-Kinetic Physical**: Technology meant to create interference or temporary damage and physical impact on space systems without physical contact. This category includes electromagnetic pulses or directed energy (laser beams or microwave bombardments) technologies.
- **Electronic**: Technology that uses radiofrequency energy to interfere with or jam the communications to or from satellites but not cause permanent physical damage.
- **Cyber**: Technology that uses software and network techniques to compromise, control, interfere or destroy computer systems that are linked to satellite operations.[1]

[*] UNIDIR acknowledges the valuable support and contribution of the Secure World Foundation to the preparation of this document.

Democratic People's Republic of Korea	Kinetic Physical	No open sources indicate development of DA-ASAT or co-orbital capabilities but its ballistic missile technology form the building blocks, should it take a decision to do so[2]
	Non-Kinetic Physical	Unknown
	Electronic	Between 2010 and 2012, reports emerged of jamming neighbouring GPS signals for days at a time, affecting many planes, ships and personal devices[3]
	Cyber	Has shown increasingly advanced offensive cyber capabilities, although not yet specifically against space-related targets
Republic of India	Kinetic Physical	Has the technological capabilities for a DA-ASAT but not tested it yet[4]
	Non-Kinetic Physical	Unknown
	Electronic	Unknown
	Cyber	Has shown increasingly advanced offensive cyber capabilities, although not yet specifically against space-related targets
Islamic Republic of Iran	Kinetic Physical	Not known to be developing DA-ASAT or co-orbital anti-satellite (ASAT) capabilities but has sufficient ballistic missile technology to develop kinetic ASAT capabilities, should it take a decision to do so[5]
	Non-Kinetic Physical	Unknown
	Electronic	Reports of certain existing capabilities, particularly against commercial satellite communications and public satellite navigation services[6]
	Cyber	Has shown increasingly advanced offensive cyber capabilities, although not yet specifically against space-related targets
People's Republic of China	Kinetic Physical	SC-19 DA-ASAT DN-2 DA-ASAT DN-3 DA-ASAT Multiple tests of technologies for close approach and rendezvous in both low earth orbit (LEO) and geostationary earth orbit (GEO), e.g. SJ 7 and Advanced Debris Removal Vehicle ("Roaming Dragon")
	Non-Kinetic Physical	Reports of certain existing capabilities[7]

	Electronic	Reports of certain existing capabilities[8] [9]
	Cyber	Reports of certain existing capabilities[10]
Russian Federation	Kinetic Physical	Co-orbital technology[11] A-235/PL-19[12]/Nudol, a rapidly maturing ground-launched ballistic missile designed to be capable of intercepting targets in LEO 78M6 Kontakt Air-launched missile (development stage) S-500 ABM air defence system (could serve a dual missile defence-ASAT purpose)
	Non-Kinetic Physical	Reports of certain existing capabilities[13]
	Electronic	Completed the development of a laser-based ASAT system on A-60, designated 1LK222 Sokol Eshelon, with plans for integration onto an airborne platform[14] R-330Zh jammer and R-381T2 ultra-high frequency (UHF) radio monitoring system for jamming[15] [16]
	Cyber	Turla malware[17]
United States of America	Kinetic Physical	ASM-135 Air-Launched DA-ASAT Midcourse Missile Defence Systems as ASAT–SM-3 variants No openly acknowledged co-orbital capabilities but has latent technological capability to develop in a short time period if it so chooses
	Non-Kinetic Physical	Reports of certain existing capabilities[18]
	Electronic	Counter Communications System Navigation Warfare programme
	Cyber	Has shown increasingly advanced offensive cyber capabilities, although not yet specifically against space-related targets

Notes

[1] "As space capabilities continue to shift towards incorporating more advanced on-board processing, all digital components, software-defined radios, packet-based protocols, and cloud-enabled high-performance computing, the attack surface for cyber-attacks is likely to increase. 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." See Brian Weeden and Victoria Samson, "Global Counterspace Capabilities: An Open Source Assessment", Secure World Foundation, April 2018, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[2] Todd Harrison, Kaitlyn Johnson and Thomas G Roberts, "Space Threat Assessment 2018", Center for Strategic and International Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180412_Harrison_SpaceThreatAssessment_FULL_WEB.pdf?0YxNhtucgT6o6g5I7yqeBaL7CB6mBZEu.

[3] "DPRK jamming GPS signals, says Seoul", *North Korea Tech*, 3 May 2012, http://www.northkoreatech.org/2012/05/03/dprkjamming-gps-signals-says-seoul/; "'North Korea jamming' hits South Korea flights", *BBC News*, 2 May 2012, http://www.bbc.com/news/world-asia-17922021; Shaun Waterman, "North Korean jamming of GPS shows system's weakness", *The Washington Times*, 23 August 2012, https://www.washingtontimes.com/news/2012/aug/23/north-korean-jamming-gps-shows-systems-weakness/.

[4] Former Defence Research and Development Organisation (DRDO) Chief and Scientific Adviser to the Defence minister, VK Saraswat, on the sidelines of the 97th Indian Science Congress in 2008 stated that India had begun developing ASAT capabilities. He said, "India is putting together building blocks of technology that could be used to neutralize enemy satellites ... . [thereby] working to ensure space security and protect our satellites. At the same time, we are also working on how to deny the enemy access to its space assets". In February 2010, speaking to the press after the Agni-III test, Saraswat said that with the successful test of the Agni-III missile, India's anti-satellite capability has been proven. He added, "With the successful testing of Agni-III, we have the propulsion system which can be used to propel a kill vehicle in the orbit. We have the capability required to guide a kill vehicle towards the satellite. We have the capability for interception of satellite. But we do not have to test because it is not our primary objective. There are repercussions of satellite interception like debris flying in the space. Today we can validate the anti-satellite technology on ground through simulation. If the nation wants, we can have it ready". See "India Readying Weapon to Destroy Enemy Satellites", *Indian Express*, 3 January 2010, http://archive.indianexpress.com/news/india-readying-weapon-to-destroy-enemy-satellites-saraswat/562776/; "India Has Anti-satellite Capability: DRDO", *Hindustan Times*, 10 February 2010, https://www.hindustantimes.com/delhi-news/india-has-anti-satellite-capability-drdo/story-qEBKLYsjsMznnZnVyCFcFI.html.

[5] Harrison, Johnson and Roberts, op. cit.

[6] In 2011, Iran claimed to have brought down a US drone, RQ-170, " … by jamming its satellite communications links and spoofing the GPS signals it received". The US government did not confirm Iran's claims. See Scott Peterson and Payam Faramarzi, "Exclusive: Iran hijacked US drone, says Iranian engineer", *The Christian Science Monitor*, 15 December 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer; Harrison, Johnson and Roberts, op. cit. In another specific case, Iran has been accused of jamming certain news broadcasts, such as that of BBC's Persian TV, in order to prevent Western media from reaching domestic viewers. See "BBC Fears Iranian Cyber-Attack over Its Persian TV Service", *The Guardian*, 14 March 2012, http://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian; Peter Horrocks, "Stop Blocking Now", *BBC News*, 14 June 2009, http://www.bbc.co.uk/blogs/theeditors/ 2009/06/stop_the_blocking_now.html in Rajeswari Pillai Rajagopalan and Daniel A Porras; "Cyber Arms Race in Space: Exploring India's Next Steps", *Issue Brief* No. 113, Observer Research Foundation, New Delhi, November 2015, https://www.orfonline.org/wp-content/uploads/2015/12/Issue-Brief_113.pdf. In another specific incident reported by Christian Science Monitor in 2011, according to an unnamed European intelligence source, Iran had "managed to 'blind' a US satellite by 'aiming a laser burst quite accurately'". See Harrison, Johnson and Roberts, op. cit.

[7] Richard D. Fisher, Jr, "China's Progress with Directed Energy Weapons", Testimony before the U.S.-China Economic and Security Review Commission hearing, "China's Advanced Weapons", Washington, DC, 23 February 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

[8] See Anthony Capaccio, "Chinese Military Suspected in Hacker Attacks on US Satellites", *Bloomberg*, 27 October 2011, http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites; "China denies it is behind hacking of US satellites", *Reuters*, 31 October 2011, http://www.reuters.com/article/2011/10/31/us-china-us-hacking-idUSTRE79U1YI20111031; Les Johnson, "Sky Alert: When Satellites Fail", *Springer*, 2013, p. 37, Google Books; Mary Pat Flaherty, Jason Samenow and Lisa Rein, "Chinese Hack US Weather Systems, Satellite Network", *Washington Post*, 12 November 2014, http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellitenetwork/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

[9] It was widely reported that "several Chinese scientists claimed to have successfully blinded a satellite in a 2005 test using a '50-100 [kilowatt] capacity mounted laser gun in Xinjiang province'". See Richard D. Fisher, Jr., "China's Progress with Directed Energy Weapons", Testimony before the U.S.-China Economic and Security Review Commission, 23 February 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf in Harrison, Johnson and Roberts, op. cit. See Vago Muradian, "China Tried To Blind U.S. Sats With Laser", *Defense News*, 25 September 2006, https://www.ar15.com/forums/general/Chi-na_Tried_To_Blind_U_S__Sats_With_Laser/5-501978/ in Harrison, Johnson and Roberts, op. cit. See Francis Harris, "Beijing secretly fires lasers to disable US satellites", *The Telegraph*, 26 September 2006, https://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html in Harrison, Johnson and Roberts, op. cit.

[10] In 2011, a report by the US-China Economic and Security Review Commission reported that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway. Though the US government did not accuse anyone outright, it did say that the nature of the attack was linked with Chinese hackers and that it was consistent with policy documents published by China's military. The severity of the attack was especially alarming because, at least in the 2008 attack the hackers demonstrated the ability to undertake all steps required to command the satellite, though in this case they stopped short of such actions. Potentially, the hackers could have stolen data, destroyed the solar panel array by redirection or even moved the satellite to cause a collision.

[11] Since 2010, Russia has been engaged in testing technologies for close approach and rendezvous operations in both LEO and GEO that could lead to a co-orbital ASAT capability. These technologies appear to be based on a Cold War-era LEO co-orbital ASAT programme. See Harrison, Johnson and Roberts, op. cit.

[12] Bill Gertz, "Russia Flight Tests Anti-Satellite Missile", *The Washington Free Beacon*, 2 December 2015, http://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/; Bill Gertz, "Russia Flight Tests Anti-Satellite Missile", *The Washington Free Beacon*, 28 May 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile/ in Harrison, Johnson and Roberts, op. cit.

[13] "Russian Engineers Finish Work on Laser Capable of Shooting Down Enemy Satellites", *Sputnik*, 25 February 2018, https://sputniknews.com/military/201802251061979166-russia-creates-airborne-antisatellite-laser/. "To challenge US spy satellites, Russia to build an anti-satellite weapon", *Xinhua*, 5 March 2018, http://www.xinhuanet.com/mil/2018-03/05/c_129822695.htm.

[14] These laser-based systems have the capability to both dazzle and blind sensors on satellites. With sufficient power, they are capable of damaging "light- or heat-sensitive physical components" on satellites. See Harrison, Johnson and Roberts, op. cit.; Arun Mathew, "Russia Completes Development of Airborne Anti-satellite Laser Weapon", *DefPost*, 26 February 2018, https://defpost.com/russia-completes-development-airborne-anti-satellite-laser-weapon/; David Cenciotti, "Russia has completed ground tests of its high-energy Airborne combat Laser System", *The Aviationist*, 5 October 2016, https://theaviationist.com/2016/10/05/russia-has-completed-ground-tests-of-its-high-energy-airborne-combat-laser-system/; "The Russian plane with laser weapons successfully passed the ground tests", *TV Zvezda*, 5 October 2016, https://tvzvezda.ru/news/opk/content/201610051309-vplh.htm.

[15] These two, along with four other jamming systems, were reportedly used to jam GPS signals in Ukraine in 2014. See Harrison, Johnson and Roberts, op. cit.

[16] According to a Russian defence industry source reported in *Sputnik*, Russia is building a new electronic warfare aircraft that can turn off electronics on military satellites and disable enemy satellites used in navigation and communication sectors. See "Source Reveals Tech Details of New Russian Anti-Satellite Warfare Plane", *Sputnik*, 9 July 2018, https://sputniknews.com/military/201807091066176858-russia-electronic-warfare-plane-satellites/.

[17] See "Turla: Spying tool targets governments and diplomats", Symantec Security Response, 7 August 2014, https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats in Harrison, Johnson and Roberts, op. cit.

[18] Marc Selinger, "DoD's Griffin Eyes Using Directed Energy for Space-Based missile Defense", *Defense Daily*, 17 April 2018, http://www.defensedaily.com/dods-griffin-eyes-using-directed-energy-space-based-missile-defense/. Melissa Olson, "History of Laser Weapon Research", Naval Surface Warfare Center, 2012, https://pdfs.semanticscholar.org/3043/1906ceb269c09ae08f68076368a183a0a27f.pdf.