SIPRI Background Paper
September 2023

THE ROLE OF SPACE SYSTEMS IN NUCLEAR DETERRENCE

NIVEDITA RAJU AND TYTTI ERÄSTÖ*

SUMMARY

● Space systems are used for multiple civilian and military purposes, including missions related to nuclear deterrence. Consequently, real and perceived military operations targeting space systems may create pathways to nuclear escalation.

China, Russia and the United States possess both nuclear weapons and counterspace capabilities, and they are at risk of being drawn into war with each other through regional conflicts and great power competition. These states have integrated space systems into their nuclear deterrence practices to varying degrees for missile early warning, communications, intelligence, surveillance and reconnaissance (ISR), and navigation. These space systems can be vulnerable to attack or interference through counterspace capabilities—including direct-ascent and co-orbital anti-satellite (ASAT) weapons, directed-energy weapons, electronic interference and cyber operations.

Each of the three states' space systems has varying strategic value. Each system is also vulnerable to the counterspace capabilities of the others. Examining space systems relevant to nuclear deterrence and assessing their vulnerabilities lays the groundwork for further analysis on escalation pathways and risk-reduction measures.

I. Introduction

The possibility of a conventional conflict escalating to the use of nuclear weapons has been discussed extensively since the early days of the cold war. This risk is currently being highlighted by regional conflicts and tensions, as well as the strategic competition between China, the Russian Federation and the United States. At the same time, the multidomain nature of contemporary warfare appears to have created new pathways to nuclear escalation. In particular, the importance of outer space and cyberspace has grown in recent decades. Modern weapons are increasingly reliant on space-based assets and digital communications technology. There is consequently the risk that warfighting on the ground, at sea and in the air could spill over to these two domains—or be triggered by dynamics there.

Focusing on one of these domains, this SIPRI Background Paper provides an overview of, first, the space systems that play a role in nuclear deterrence and, second, counterspace capabilities—that is, the means and methods by which space systems can be attacked. While there is no common understanding among states of the term 'weapon' in the space context, the term 'counterspace capabilities' is used here to refer to both capabilities and techniques that can disrupt, damage or destroy space systems, including offensive, defensive and enabling technologies that facilitate target identification.

This paper provides the basis to explore nuclear escalation risks in connection with the space domain, with a focus on China, Russia and the USA. These three states possess both nuclear weapons and counterspace capabilities and are at risk of being drawn into war with each other through regional conflicts and great power competition. All of them rely on space systems for various civilian and military functions, including those related to nuclear weapons. Yet, in contrast to the more widely reported modernization of their nuclear arsenals, these states' involvement in arms race dynamics in outer space, particularly the ways in which these dynamics intersect with the nuclear domain, remains less understood. This paper details existing space systems and counterspace capabilities, indicating their strategic significance and assessing their vulnerabilities. This lays the groundwork for further analysis on escalation risks and ways to reduce them. Such risks are not limited to China, Russia and the USA, so the analysis also seeks to inform future research on other states that are engaged in similar dynamics.

Section II of this paper describes space systems that play a role in the nuclear deterrence practices of China, Russia and the USA. The analysis

* The authors would like to thank the Ministry of Foreign Affairs of the Netherlands, which generously provided funding for this project.

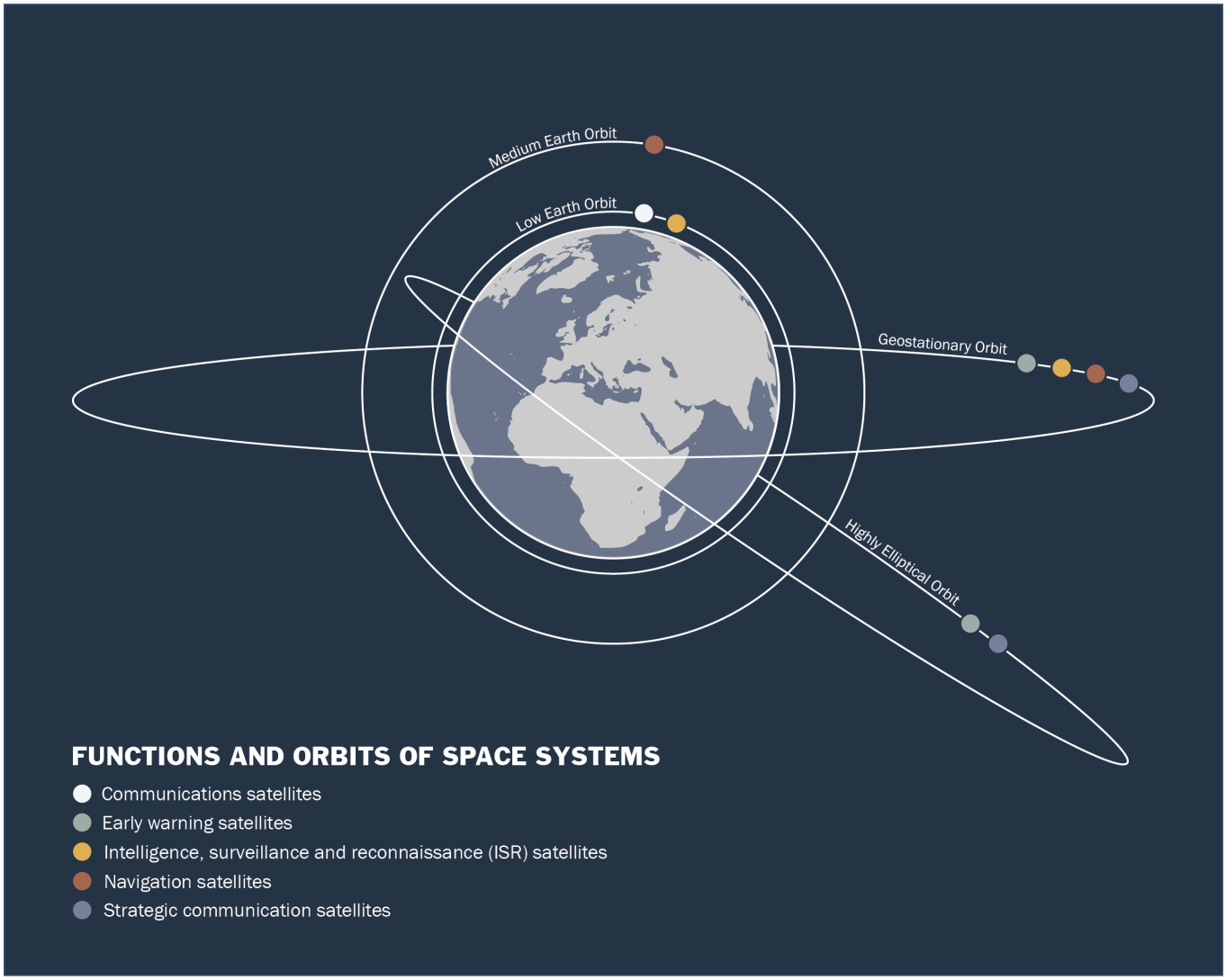

Figure 1. Functions and orbits of space systems

both sheds light on the multiple functions of space systems and provides indications of the strategic value of particular types of space assets for the three states. This is followed in section III by a brief overview of these states' known counterspace capabilities. On this basis, section IV assesses the vulnerabilities of strategically relevant space systems, taking into account not only existing capabilities but also considering likely inhibitions to conducting attacks that either generate debris or involve high risks of escalation. The paper ends in section V by summarizing the findings and discussing the implications for nuclear risk reduction.

II. Space systems relevant to nuclear deterrence

The space domain has long been used to support nuclear deterrence practices through satellite-based intelligence, surveillance and reconnaissance (ISR), missile early warning, and strategic communications. It is therefore no coincidence that the two states that possess the most nuclear weapons—Russia (succeeding the Soviet Union) and the United States—have traditionally been the leading spacefaring states. The USA owns the majority

of operational satellites currently in orbit, followed by Russia.[1] In recent years, however, the number of actors in space has increased, with China in particular expanding its activities. This change has coincided with growing strategic competition between China and the USA and worsening tensions between Russia and the USA.

This section describes and compares the role of space systems—including satellites performing functions related to missile early warning, communications, ISR and navigation—in the three countries' nuclear deterrence practices. (On functions and orbits of space systems, see figure 1.) Previous literature has highlighted the strategic importance of satellites in geostationary orbit (GEO) and highly elliptical orbit (HEO) in particular.[2] However, as noted below, satellites in other orbits—low earth orbit (LEO) and medium earth orbit (MEO)—are also becoming increasingly relevant for nuclear deterrence. (On types of orbit, see box 1.)

Missile early warning

Early-warning satellites are normally placed in GEO or HEO, from where they can cover wide areas of the earth's surface. These satellites use infrared sensors to detect the heat from ballistic missiles during their boost phase. They can thus provide the first indication of a potential nuclear attack. Combined with radar-based information on the trajectory of the incoming missile, this could trigger a retaliatory nuclear strike before the adversary's missiles reach their target. By increasing the time in which to make a decision in such situations, early-warning satellites play a crucial role in nuclear command, control and communications (NC3), particularly for countries such as Russia and the USA that maintain a 'launch-on-warning' posture (i.e. a readiness to initiate nuclear retaliation right after the detection of incoming adversary missiles, before they reach their targets).[3]

In addition to NC3, early-warning satellites play a critical role in missile defence, which depends on near real-time detection of missile launches to intercept incoming missiles before they reach their destination. With the expansion of both strategic and regional missile defences in recent decades, early-warning satellites increasingly have non-nuclear missions.[4] This is the case particularly for the USA, which deploys the largest number of missile defences in the world. These include the Ground-based Midcourse Defense

[1] UN Office for Outer Space Affairs, 'Online index of objects launched into outer space', <https://www.unoosa.org/oosa/osoindex/search-ng.jspx>; Union of Concerned Scientists (UCS), 'UCS Satellite Database', 1 Jan. 2023, <https://www.ucsusa.org/resources/satellite-database>; and McDowell, J. C., 'GCAT: General Catalog of Artificial Space Objects', GCAT Release 1.4.0, 14 Apr. 2023, <http://nssdc.space.planet4589.com/space/gcat/web/lvs/stages/index.html>.

[2] Acton, J. M., MacDonald, T. D. and Vaddi, P., *Reimagining Nuclear Arms Control: A Comprehensive Approach* (Carnegie Endowment for International Peace: Washington, DC, Oct. 2021). See also Acton, J. M. (ed.), *Entanglement: Russian and Chinese Perspectives on Non-nuclear Weapons and Nuclear Risks* (Carnegie Endowment for International Peace: Washington, DC, 2017).

[3] US Strategic Command uses the term 'launch under attack' to describe US nuclear posture, which, while almost synonymous to 'launch-on-warning', implies a higher degree of confidence that an attack is actually taking place. See von Hippel, F. N., 'Biden should end the launch-on-warning option', *Bulletin of the Atomic Scientists*, 22 June 2021.

[4] See Stone, C., 'Enhanced space-based missile tracking', *Air & Space Forces*, 7 Oct. 2022. See also Grego, L., 'Outer space and crisis risk', eds C. Steer and M. Hersch, *War and Peace in Outer Space: Law, Policy and Ethics* (Oxford University Press: Oxford, 2020), p. 274.

Box 1. Types of orbit

Space systems use different orbits based on their intended function. Each orbit provides varying advantages for systems relevant to nuclear deterrence.

A low earth orbit (LEO) has an altitude between 100 kilometres and 2000 km, while a medium earth orbit (MEO) has an altitude between 2000 km and 24 000 km. The geostationary orbit (GEO) is a circular orbit at an altitude of 35 786 km. Satellites in GEO appear to be in a fixed position in relation to an observer on earth. A highly elliptical orbit (HEO) ranges in altitude from 600 km up to 40 000 km. The term 'HEO' is sometimes used interchangeably with 'Molniya orbit' in reference to the Soviet Union's Molniya satellite series, which was placed in an HEO.

Satellites in GEO can cover wide areas of the earth's surface simultaneously. This makes them optimal not only for broadcasting and strategic communications, but also for detecting ballistic missile launches using infrared sensors.[a] HEO is used for the same purposes as GEO but is more suitable for observation of the northern hemisphere as it enables coverage of high-latitude areas.[b] The ability to provide global sensor coverage makes both GEO and HEO particularly relevant for nuclear deterrence. Satellites in these orbits are used for early warning and nuclear command, control and communications (NC3).

In contrast, the detailed imagery and strong signals provided by space systems operating in LEO are useful for intelligence, surveillance and reconnaissance (ISR) as well as communications functions for various military operations. Such information also makes ISR satellites useful for nuclear planning and targeting. Satellites in MEO are mostly used for navigation. They can facilitate the tracking of targets and can guide precision-strike weapons. Some satellites in MEO carry sensors used to detect nuclear detonations.

[a] Wright, D., Grego, L. and Gronlund, L., *The Physics of Space Security: A Reference Manual* (American Academy of Arts and Sciences: Cambridge, MA, May 2005), p. 43.

[b] Wright et al. (note a), p. 43.

(GMD) system, which covers US territory, as well as various regional defences that the USA often operates jointly with its allies.[5]

The USA is the only country that discloses details of its space-based early-warning system.[6] It first deployed early-warning satellites in the 1970s to complement its radar-based system to detect strategic missile launches by the Soviet Union. In the 1980s it responded to the proliferation of ballistic missiles by equipping its early-warning system to also detect and track shorter-range ballistic missiles.[7] Today, US early-warning satellites scan the earth providing a '24/7 global strategic missile warning capability'.[8] These satellites are mainly located in GEO, with some also placed in HEO.[9]

The USA is currently replacing its cold war-era Defence Support Program (DSP) early-warning system with the Space-Based Infrared System (SBIRS), which, according to unclassified reports, consists of six satellites in GEO and additional sensors on satellites in HEO.[10] At the same time, the USA has been considering strategies for disaggregation of the space-based components of its early-warning system, intending to distribute its functions among a larger number of satellites in different orbits, including LEO and MEO.[11] These efforts seek to limit the vulnerability of the current early-warning

[5] Center for Arms Control and Non-proliferation, 'US ballistic missile defense', Fact sheet, 12 June 2023.

[6] US Space Force, 'Space Based Infrared System', Fact sheet, Mar. 2023.

[7] Burr, W. (ed.), *Launch on Warning: The Development of US Capabilities, 1959–1979*, National Security Archive Electronic Briefing Book no. 43 (George Washington University, National Security Archive: Washington, DC, Apr. 2001); and Stone (note 4).

[8] US Space Force (note 6).

[9] US Space Force (note 6). See also Villareal Dean, M., 'US space-based nuclear command and control: A guide', Center for Strategic and International Studies, 13 Jan. 2023.

[10] US Space Force (note 6).

[11] Hitchens, T., 'Space Force phasing out missile warning from GEO, will focus on lower orbits', Breaking Defense, 21 Sep. 2022.

system, which is comprised of a few high-value satellites that, in the words of a US Space Force official, make for 'big, fat, juicy targets' for attacks.[12] The intention to disaggregate more systems in lower orbits reflects the US priority of achieving 'resiliency' in its space systems.[13]

Over the next decade, the USA intends to further augment its space-based missile-tracking capability with the Next-Generation Overhead Persistent Infrared (Next-Gen OPIR) programme, which, a US official argues, will have 'exceptional resilience to prevail against enemy counter-space threats'.[14] In addition, the USA is developing a 'tracking layer' of satellites in LEO, including the Hypersonic and Ballistic Tracking Space Sensor (HBTSS) programme.[15] The HBTSS would be cued by early-warning satellites to track and intercept incoming hypersonic glide vehicles—a task that would be beyond the capacity of existing missile defences, particularly if used against long-range hypersonic weapons.

There is little state-sourced data on the space segments of the Russian early-warning system. Historically, while the coverage of the US early-warning system was global, that of the Soviet system was not; instead, it seems to have been largely limited to the northern hemisphere, where missile threats against the country were most likely to appear.[16] Like the USA, the Soviet Union began to deploy early-warning satellites in the 1970s.[17] While these also included satellites in GEO, HEO was particularly suitable for the Soviet Union because the country's territory extended above the Arctic circle.[18]

The planned system and its implementation encountered technical difficulties in the following decades.[19] By 2002 the entire Russian early-warning system—including ground-based radars—had deteriorated to an extent that questioned its reliability as a basis for the country's launch-on-warning posture.[20] The technical capacity of Russia's early-warning system was also called into question in 2006 due to its apparent inability to track missile launches by North Korea.[21]

Russia seems to have undertaken efforts to modernize the system over the past two decades, including developing a new generation of satellites in the

[12] Erwin, S., 'STRATCOM Chief Hyten: "I will not support buying big satellites that make juicy targets"', SpaceNews, 19 Nov. 2017. See also Sankaran, J., '"Big, fat, juicy targets"—The problem with existing early-warning satellites. And a solution', *Bulletin of Atomic Scientists*, 30 Sep. 2019.

[13] Wilson, R. S., 'Space Force budget brief: New priorities and long-term developments towards a new architecture', Issue brief, Aerospace Corporation, Center for Space Policy and Strategy, Issue Brief, June 2023, p. 5.

[14] US Space Force, Space Systems Command, 'Next-Generation Overhead Persistent Infrared Program selects mission payload suppliers', Media release, 1 Mar. 2022.

[15] US Department of Defense, 'Missile Defense Agency officials hold a press briefing on President Biden's fiscal 2024 missile defense budget', 14 Mar. 2023. See also Sayler, K. M., 'Hypersonic missile defense: Issues for Congress', In Focus, US Congress, Congressional Research Service, 2 May 2023.

[16] Podvig, P., 'History and the current status of the Russian early-warning system', *Science and Global Security*, vol. 10, no. 1 (2002), pp. 22–23.

[17] Podvig (note 16), pp. 26, 39, 40; and Hendrickx, B., 'EKS: Russia's space-based missile early warning system', Space Review, 8 Feb. 2021.

[18] Podvig, P. (ed.), *Russian Strategic Nuclear Forces* (MIT Press: Cambridge, MA, 2004), pp. 428–30.

[19] Podvig (note 16), pp. 26, 39, 40.

[20] Podvig (note 16), pp. 26, 39, 40.

[21] Podvig, P., 'Did Russian early-warning radars see North Korean missiles?', Russian Strategic Nuclear Forces, 5 July 2006; and Pollack, J., 'Russia eyes North Korea', Arms Control Wonk, 7 Apr. 2006.

2000s.[22] Russian officials have also referred to this modernization process.[23] In 2019 the Russian Ministry of Defence argued that the country's new satellites 'significantly increased our ability to guarantee detection of ballistic missile launches'.[24] Russia's deputy defence minister reportedly likened the new early-warning satellites to the USA's SBIRS, suggesting that their coverage would be global.[25] However, while the modernization of Russia's early-warning system is still under way, it appears that its early-warning satellites have not thus far reached the maturity of SBIRS.[26]

The role of satellites in the Chinese early-warning system is even less clear than in the case of Russia; there is no public state-sourced information on China's early-warning satellites or their development. Historically, China has maintained a low level of readiness of its nuclear forces, which is why the early detection of missile launches has not been as essential for its nuclear posture as in the case of Russia and the USA.[27]

According to the US Department of Defense (DOD), China began developing space-based early-warning components in 2013, having previously relied on ground-based radars for early warning.[28] These satellites may also be used for intelligence purposes.[29] In 2022 the US DOD estimated that China had 'at least three early warning satellites in orbit'.[30] China officially declares the function of these satellites to be 'communication'.[31] However, this does not exclude the possibility that they are also used for early warning, as satellites often serve multiple functions, such as missile detection and strategic communications.

In 2019 China and Russia reportedly commenced cooperation on early-warning systems; there is some speculation that this could lead to joint integrated use of Russia's early-warning system.[32] In addition to ground-

[22] Podvig, P. and Zhang, H., *Russian and Chinese Responses to US Military Plans in Space* (American Academy of Arts and Sciences: Cambridge, MA, 2008), p. 7.

[23] TASS, 'Russia creates unified space system to detect ballistic missile launches', 9 Oct. 2014; and Tikhonov, A., [To ensure that we retain air supremacy], Interview with Colonel General Sergei Surovikin, *Redstar*, 3 July 2020, p. 4 (in Russian).

[24] Russian Ministry of Defence, [Chief of the General Staff of the Armed Forces of the Russian Federation, Army General Valeri Gerasimov, met with representatives of the military-diplomatic corps accredited in Russia], 18 Dec. 2019 (in Russian, author translation).

[25] Hendrickx (note 17).

[26] Hendrickx (note 17).

[27] Kristensen, H. M. and Korda, M., 'Chinese nuclear forces', *SIPRI Yearbook 2023: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2023), pp. 284–85; and Cunningham, F. S., 'The unknowns about China's nuclear modernization program', *Arms Control Today*, vol 53, no. 5 (June 2023).

[28] US Department of Defense (DOD), *Military and Security Developments involving the People's Republic of China 2021*, Annual report to the US Congress (DOD: Washington, DC, 2021), pp. 93–94.

[29] Gunter's Space Page, 'TJS 2, 5, 6 (Huoyan-1 ?)', 14 Jan. 2023; and Gunter's Space Page, 'TJS 3 / TJS 3 subsatellite', 14 Jan. 2023.

[30] US Department of Defense (DOD), *Military and Security Developments involving the People's Republic of China 2022*, Annual report to the US Congress (DOD: Washington, DC, 2022), p. 99.

[31] E.g. see the registration of the satellites TJS-2 and TJS-3 in United Nations, Committee on the Peaceful Uses of Outer Space (COPUOS), 'Registration data on space objects launched by China', ST/SG/SER.E/856, 21 Aug. 2018, p. 9; and United Nations, Committee on the Peaceful Uses of Outer Space (COPUOS), 'Registration data on space objects launched by China', ST/SG/SER.E/898, 15 July 2019, p. 36.

[32] Chan, M., 'Vladimir Putin says Russia is helping China build a missile early warning system', *South China Morning Post*, 4 Oct. 2019; and Korolev, A., 'China–Russia cooperation on missile attack early warning systems', East Asia Forum, 20 Nov. 2020.

based radars, Russian assistance to China in this context might include space-based sensors.[33]

In 2021 the US DOD claimed that China's interest in space-based early warning, alongside its nuclear build-up and what the USA views as the increased readiness of China's nuclear forces, is connected to an emerging launch-on-warning posture similar to that of Russia and the USA.[34] Other observers share the view that China's recent nuclear modernization has included adjustments to its alert levels.[35] However, this does not necessarily mean a shift to a launch-on-warning posture, even though the adjustments could pave the way for such a shift in the future.[36] China has rejected speculation about a change in its nuclear posture, reiterating its policy of nuclear restraint and calling on all nuclear-armed states to reduce the alert levels of their nuclear forces.[37]

Communications

China, Russia and the USA all use GEO satellites for military satellite communications (satcom). Alongside support for non-nuclear military operations and diplomatic missions, satcom constitutes a key element of nuclear deterrence: strategic communications facilitate NC3 by relaying messages within a state's nuclear command chain. Communications satellites also include data-relay satellites, which facilitate faster transmission of large quantities of data between the space and ground segments of space systems, for both civilian and military use.

The USA publicly acknowledges that it uses specific space systems for transmission of presidential orders to launch nuclear weapons.[38] It is currently taking steps to split communications for nuclear and non-nuclear missions into different space systems.[39] Satellites are reportedly also part of the Russian strategic communications system through which nuclear weapon use would be authorized.[40] It is likely that China's early-warning satellites are equipped to conduct similar strategic communications functions for nuclear use.

[33] US Department of Defense (DOD), *Military and Security Developments involving the People's Republic of China 2020*, Annual report to the US Congress (DOD: Washington, DC, 2020), p. 89.

[34] US Department of Defense (note 28), pp. 93–94.

[35] Kristensen and Korda (note 27), pp. 284–85; and Zhao, T., *Tides of Change: China's Nuclear Ballistic Missile Submarines and Strategic Stability* (Carnegie Endowment for International Peace: Washington, DC, 2018).

[36] Cunningham (note 27).

[37] Li, S., Chinese Ambassador for Disarmament Affairs, Statement, Thematic discussion on nuclear weapons, UN General Assembly, First Committee, 19 Oct. 2022; and 2026 Non-Proliferation Treaty Review Conference, Preparatory Committee, 'Nuclear risk reduction', Working paper by China, NPT/CONF.2026/PC.I/WP.30, 2 Aug. 2023. See also Kulacki, G., 'China rejects policy of nuclear launch on warning of an incoming attack', Union of Concerned Scientists, 28 Oct. 2019.

[38] US Space Force, Space Operations Command, 'Advanced Extremely High Frequency System (AEHF)', Aug. 2021; and US Space Force, 'MILSTAR satellite communications system', Fact sheet, Oct. 2020.

[39] US Space Force, Space Systems Command, 'Evolved strategic satcom program uses innovative competition to drive acquisition of threat-focused software', Media release, 2 May 2023; and Hitchens, T., 'In a $3 billion bet, Space Force envisions tactical anti-jam satcom keeping enemy EW at bay', Breaking Defense, 22 Mar. 2023.

[40] Yarynich, V. E., *C3: Nuclear Command, Control Cooperation* (Center for Defense Information: Washington, DC, May 2003), p. 150; and Hendrickx (note 17).

In addition to strategic communications satellites in GEO, the three states also have other civilian and military communications satellites in LEO that are unlikely to have any nuclear weapon-related missions. Moreover, commercial communications satellites in LEO—thousands of which have been launched in megaconstellations in recent years—may serve military purposes. For example, the Starlink satellites launched by SpaceX, a US company, have provided communications services for civilian and military users in Ukraine. In response, Russia has reportedly attempted to jam Starlink satellites.[41] Russian state representatives have also argued that these satellites 'may become a legitimate target for retaliation'.[42] While such statements are meant to restrict the use of Starlink in Ukraine, it is unclear whether Russia would be ready to conduct a kinetic strike on these satellites, which would be unprecedented and highly provocative (as discussed in section IV).[43]

Intelligence, surveillance and reconnaissance

One of the earliest military uses of space systems was for observation and information collection, also known as intelligence, surveillance and reconnaissance. The ability to gather intelligence on adversaries without infringing upon their territorial sovereignty has made space-enabled ISR valuable to many states, including China, Russia and the USA. ISR satellites enable the collection of information on rival states' nuclear facilities, capabilities and related observable activities, and thus also facilitate counterforce targeting (i.e. directing nuclear weapons against military targets such as the adversary's nuclear forces and NC3 systems). Early examples of space-based ISR include the US Corona programme from the 1960s and the Soviet/Russian Yantar series from the 1980s, which provided information on missile capabilities and sites of interest.[44] In addition to their importance for nuclear deterrence, ISR satellites form a key part of the 'national technical means' of verification—intelligence sources used to monitor compliance with bilateral arms control agreements between the Soviet Union or Russia and the USA dating back to the 1970s.[45]

The importance of space-based ISR capabilities has risen in recent years with the evolution of precision-strike weapons, whose effectiveness depends on accurate and timely information on targets. Some observers have argued that nuclear deterrence relationships are being revolutionized particularly through the deployment of constellations of surveillance satellites equipped

[41] Insinna, V., 'SpaceX beating Russian jamming attack was "eyewatering": DoD official', Breaking Defense, 20 Apr. 2022; and Horton, A., 'Russia tests secretive weapon to target SpaceX's Starlink', *Washington Post*, 18 Apr. 2023.

[42] United Nations, General Assembly, Open-ended Working Group on Reducing Space Threats, 2nd session, Statement by Russia, 12 Sep. 2022, p. 2.

[43] Raju, N. and Saalman, L., 'The space–cyber nexus', *SIPRI Yearbook 2023* (note 27), pp. 485–88; and Zarkan, L. C., 'Commercial space operators on the digital battlefield', Cybersecurity and Outer Space Essay no. 8, Centre for International Governance Innovation (CIGI), 29 Jan. 2023.

[44] US National Reconnaissance Office, 'Pioneer spy satellites to be lauded', Press release, 24 May 1995; and Podvig and Zhang (note 22), p. 8.

[45] E.g. US Department of State, 'Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms (SALT II): Narrative', [n.d.]. See also Bateman, A., 'Trust but verify: Satellite reconnaissance, secrecy and arms control during the Cold War', *Journal of Strategic Studies*, vol. 46, no. 5 (8 Jan. 2023).

with synthetic-aperture radars (SARs).[46] SARs equipped with new data-processing techniques may facilitate precision strikes against mobile missile launchers that were traditionally considered highly likely to survive nuclear counterforce attacks.[47]

Depending on the type of intelligence that a state seeks to obtain—such as imagery intelligence (IMINT) or signals intelligence (SIGINT) among others—the space component of ISR systems can be located in different orbits.[48] Most of the ISR satellites currently operated by China, Russia and the USA are in LEO. For example, earth-observation satellites in LEO can collect IMINT. However, some satellites in GEO and HEO can also serve ISR functions. For example, early-warning satellites in GEO that detect missile launches can also have multiple and overlapping ISR functions.

The USA has long had a sophisticated space-based ISR capability. Its ISR satellites, together with satellite-based navigation (see below), provided critical advantages in precision-strike technology during US-led military operations in the post-cold war period. China, too, has a significant space-enabled ISR network, as the majority of its satellites support ISR functions.[49] While Russia also places high military value on its space-based ISR capabilities, it operates fewer ISR satellites than China and the USA.[50] Western sanctions imposed on Russia since 2014 seem to have had an impact on the country's space industry, including ISR satellites.[51]

A notable development in space-enabled ISR is the technological advances made in artificial intelligence (AI). It is difficult to estimate the extent of these developments among the three states. Nonetheless, because advances in machine learning and autonomy have the ability to improve the processing and analysis of data obtained from ISR satellites, AI can be expected to influence military decision-making and response times.[52] According to some estimates, this could enable future 24/7 monitoring of critical sites such as the bases of nuclear-powered ballistic missile submarines (SSBNs) and the bases and patrol areas of road-mobile intercontinental ballistic missiles (ICBMs).[53]

[46] Lieber, K. A. and Press, D. G., 'The new era of counterforce: Technological change and the future of nuclear deterrence', *International Security*, vol. 41, no. 4 (spring 2017).

[47] Lieber and Press (note 46).

[48] US Office of the Director of National Intelligence, 'What is intelligence?', [n.d.].

[49] For an overview of Chinese earth-observation satellites, and initiatives to further expand see Guo, X., 'Chinese satellite program', ed. K.-U. Schrogl, *Handbook of Space Security: Policies, Applications and Programs* (Springer: 2020), pp. 1395–96.

[50] Chekinov, S. A. and Bogdanov, S. G., 'The nature and content of a new-generation war', *Military Thought*, vol. 22, no. 4 (Dec. 2013), p. 16.

[51] Luzin, P., 'Russia's space satellite problems and the war in Ukraine', Eurasia Daily Monitor, 24 May 2022; and Hallgren, H., Westman, J. and Wårlind, A. M., *Ryssland i rymddomänen: Från Sputnik till sanktioner—Ett försvars- och säkerhetsperspektiv* [Russia in the space domain: From Sputnik to sanctions—A defence and security perspective], Swedish Defence Research Agency (FOI) Report no. FOI-R--5340--SE (FOI: Stockholm, Dec. 2022), p. 72.

[52] Boulanin, V. et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI: Stockholm, 2020), pp. 25–26.

[53] Zhao, T. and Stefanovich, D., *Missile Defense and the Strategic Relationship among the United States, Russia, and China* (American Academy of Arts and Sciences: Cambridge, MA, 2023), p. 37.

Navigation

A global navigation satellite system (GNSS) provides position, navigation and timing (PNT) services for both civilian and military purposes. China, Russia and the USA each has independent GNSS capabilities, including the widely known US-owned Global Positioning System (GPS). Satellites for navigation are mostly located in MEO, although China's BeiDou Navigation Satellite System also uses GEO.

GNSS was originally developed in the 1960s by the USA for military purposes to improve the navigation of SSBNs.[54] Together with ISR satellites, GPS was later key to enabling conventional precision-strike technology, and it continues to be used for this purpose.[55] Alongside PNT, the US constellation of GPS satellites has an additional function of identifying whether a nuclear detonation has occurred.[56] This function is served by sensors on both GPS satellites and also the reconnaissance satellites in the early-warning system, again exhibiting the overlapping and multifunctional uses of space systems.[57]

Indeed, the many uses of GNSS evidently led China and Russia to each develop its own GNSS capabilities. After the Third Taiwan Strait Crisis, in 1996, China claimed that the USA had disrupted Chinese use of GPS and that this interference caused its missiles to fail to reach their intended test targets.[58] It has been suggested that this was a driver for Chinese development of its GNSS, BeiDou.[59] The first phase of satellite launches for BeiDou began in 2000, and the third phase became fully operational in 2020. China intends the next, fourth generation of BeiDou to ensure a backup design and strategy that can enable the elimination of 'weak links' and 'enhance system reliability'.[60] BeiDou is probably used for targeting, specifically enabling strikes from both ballistic and cruise missiles.[61]

Russia's Global Navigation Satellite System (GLONASS) became fully operational in 1995.[62] In the years that followed, the programme's funding was reduced and it suffered from technical degradation, until efforts to renew and modernize the system were initiated in the early 2000s.[63] While the system is now restored and reportedly provides global coverage, Western sanctions since 2014 have caused setbacks.[64] However, GLONASS

[54] Ceruzzi, P. E., *GPS* (MIT Press: Cambridge, MA, 2018), pp. 37–45; Aerospace Corporation, 'A brief history of GPS', [n.d.]; and Archus, D., 'How do the submarines navigate underwater?', Naval Post, 13 May 2021.

[55] Neuneck, G. and Alwardt, C., 'The revolution in military affairs, its driving forces, elements and complexity', Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) Working Paper no. 3, May 2008; and Martin, J.-C., 'Position, navigation, and timing for security', ed. Schrogl (note 49), p. 801.

[56] Villareal Dean (note 9), p. 4.

[57] Villareal Dean (note 9), p. 4.

[58] Chan, M., '"Unforgettable humiliation" led to development of GPS equivalent', *South China Morning Post*, 13 Nov. 2009.

[59] Chan (note 58).

[60] China Satellite Navigation Office, 'Development of the BeiDou Navigation Satellite System (Version 4.0)', Dec. 2019, p. 8.

[61] Thomas-Noone, B., 'Tactical nuclear weapons in the modern nuclear era', Lowy Institute, 29 Sep. 2016.

[62] Roscosmos, Information and Analysis Centre for Positioning, Navigation and Timing (IAC PNT), 'About Glonass', [n.d.].

[63] Roscosmos (note 62); and Hallgren et al. (note 51), pp. 126–27.

[64] Hallgren et al. (note 51), pp. 126–27.

is still highly valued by Russia for a number of military functions, including guidance for precision-strike weapons. Some also suggest that, like the USA, Russia also uses GLONASS to detect nuclear detonations and that it collects targeting data on behalf of the Russian Navy.[65]

Given its multiple strategic uses, Russian military experts have highlighted GLONASS as a potential target for counterspace attacks by adversaries.[66] Following the full-scale invasion of Ukraine in 2022, Russia may be seeking alternate, terrestrial-based sources for navigation due to concerns that GLONASS might be targeted by adversaries.[67] Earlier Russian media reports had indicated that Russia was preparing ground-based backups to GLONASS, in case of possible jamming.[68]

China and Russia have deepened cooperation on satellite navigation, exploring the compatibility and interoperability of systems.[69] While their cooperation appears to focus on civilian use, integration of the systems would also result in greater GNSS accuracy for the military uses of both states.

While information on the guidance systems of nuclear weapons is highly classified, GNSS may be used to support missile guidance alongside other guidance systems such as inertial navigation.[70] For example, according to some sources, GLONASS contributes to the guidance of Russia's RS-26 Rubezh ICBM as well as its non-strategic dual-capable weapons (which can carry conventional or nuclear payloads), such as the Zircon sea-launched hypersonic cruise missile, the 9K720 Iskander short-range ballistic missile and the Kh-101/Kh-102 cruise missile.[71] Similarly, one of these US-based sources suggests that China's Julang-3 (JL-3) submarine-launched ballistic missile (SLBM) uses BeiDou, whereas the Dong Feng-41 (DF-41) ICBM and several Chinese dual-capable missiles use GPS as part of their guidance systems.[72] In the case of the USA, GPS may also be used as additional guidance for the B61-12 gravity bomb.[73] However, none of these countries is likely to make the guidance systems of its nuclear weapons entirely dependent on satellites due to their vulnerability to interference.

[65] Hendrickx, B., 'The secret payloads of Russia's Glonass navigation satellites', Space Review, 19 Dec. 2022.

[66] E.g. Selivanov, V. V. and Ilyin, Yu. D., 'Choosing priorities in developing kinetic energy weapons for military conflicts', *Military Thought*, vol. 26, no. 4 (Dec. 2017).

[67] Cozzens, T., 'Russia expected to ditch GLONASS for Loran in Ukraine invasion', GPS World, 17 Feb. 2022.

[68] Krivoruchek, A., [The Scorpion system will replace GLONASS], *Izvestia*, 6 Aug. 2013 (in Russian).

[69] BeiDou Navigation Satellite System, 'Agreement on China–Russia intergovernmental cooperation on satellite navigation of [*sic*] signed in Beijing', 7 Nov. 2018.

[70] Brockmann, K. and Stefanovich, D., *Hypersonic Boost-glide Systems and Hypersonic Cruise Missiles: Challenges for the Missile Technology Control Regime* (SIPRI: Stockholm, Apr. 2022), p. 18.

[71] Missile Defense Advocacy Alliance, 'RS-26 Rubezh', 19 Sep. 2018; Peck, M., 'Putin's "invincible" missile has a very common problem', Insider, 21 Feb. 2023; Missile Threat, '9K720 Iskander (SS-26)', Center for Strategic and International Studies, 2 Aug. 2021; and Missile Threat, 'Kh-101 / Kh-102', Center for Strategic and International Studies, 31 July 2021.

[72] Missile Defense Advocacy Alliance, 'JL-3', May 2023; and Missile Defense Advocacy Alliance, 'DF-41', Jan. 2023.

[73] See e.g. Kristensen, H. M., 'The B61 Life-Extension Program: Increasing NATO nuclear capability and precision low-yield strikes', Federation of American Scientists Issue Brief, June 2011.

III. Counterspace capabilities

Given their predictable orbits and lack of cost-effective built-in defences, satellites can be targeted through various means, creating a vulnerability that rivals can exploit.[74] Thus, in parallel with the increased military importance of space systems in recent years, there has also been a renewed interest in the development and testing of various counterspace capabilities. In addition to kinetic anti-satellite (ASAT) weapons, which target satellites through motion-based physical destruction, space systems and their various components can also be incapacitated through non-kinetic means.

Perhaps the most visible demonstrations of counterspace capabilities have been kinetic, specifically 'destructive' or debris-generating ASAT weapon tests, not only by China, Russia and the United States but also by India.[75] Apart from satellites, counterspace capabilities can target the ground segment of space systems (e.g. ground stations and receivers), the data links that connect satellites with the ground segment, or even supporting systems (e.g. land-based sensors and radars or data-relay satellites that enable communication with military satellites). While ground-based components of space systems are vulnerable to attacks by conventional means (e.g. artillery, missiles or uncrewed aerial vehicles), these are not necessarily categorized as counterspace capabilities. For example, Russia claims to have destroyed a Starlink satellite communications station in Ukraine with artillery.[76] To date, only non-kinetic counterspace capabilities have been used to disrupt or attack space systems (see below).

For China and Russia, one key driver for the development of counterspace capabilities is arguably concern that US missile defences might ultimately undermine their nuclear deterrents. Since withdrawing from the bilateral 1972 Treaty on the Limitation of Anti-Ballistic Missile Systems (ABM Treaty) in 2002, the USA has expanded both its strategic and theatre missile defences.[77] In principle, counterspace capabilities could be used to counter the USA's existing ground-based missile defence systems by targeting early-warning satellites, on which the systems essentially depend. The USA has also kept open the option of developing space-based missile defences, which had been banned by the ABM Treaty.[78] Since the interceptor missiles of a hypothetical space-based missile defence system would be likely to be placed in LEO, they would be vulnerable to attack by counterspace capabilities. Further, all strategic mid-course missile defence systems have inherent ASAT capabilities, as their interceptor missiles—which target incoming mis-

[74] ed. Acton (note 2), p. 3.

[75] Raju, N., 'A proposal for a ban on destructive DA-ASAT testing: A role for the EU?', Non-Proliferation and Disarmament Papers no. 74, EU Non-Proliferation and Disarmament Consortium, Apr. 2021, pp. 3–5; and Porras, D., 'Creeping towards an arms race in outer space', *SIPRI Yearbook 2020: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2020), p. 513.

[76] Sputnik, 'Russian forces destroy Starlink communication station near Artemovsk [Bakhmut]', 2 July 2023; and TASS, 'Ukrainian UAV control center, Starlink station hit in airstrike on Dnieper right bank' 15 July 2023.

[77] Soviet–US Treaty on the Limitation of Anti-Ballistic Missile Systems (ABM Treaty), signed 26 May 1972, entered into force 3 Oct. 1972, not in force from 13 June 2002, *United Nations Treaty Series*, vol. 944 (1974); and Korda, M. and Erästö, T., 'Time to factor missile defence into nuclear arms control talks', SIPRI, 30 Sep. 2021.

[78] Acton et al. (note 2), pp. 71–73.

siles at the highest point of their trajectory, in space—could be repurposed to target satellites.[79] Hence, Chinese and Russian interest in ASAT weapons can also be seen as a response to US assertions of space dominance, to which the large number of US missile defence systems is partly contributing.

This rest of this section describes the counterspace capabilities of China, Russia and the USA based on available estimates, with the caveat that state-sourced information on such capabilities is limited. In addition to kinetic ASAT weapons, which can physically destroy targets, it describes non-kinetic means of attack such as electronic interference (i.e. jamming, spoofing and meaconing), directed-energy weapons and cyber operations.

Direct-ascent anti-satellite weapons

Direct-ascent anti-satellite (DA-ASAT) weapons are interceptors launched from earth into space to target satellites. While they have never been used against another state's satellite, China, Russia and the USA have each developed DA-ASAT weapons and demonstrated this capability by destroying their own satellites. The USA conducted several DA-ASAT tests between the 1950s and 1980s, although the first successful destructive test was conducted only in 1985.[80] While the Soviet Union pursued research and development (R&D) of ASAT technologies, its focus began with co-orbital systems in the 1950s (see below).[81] After the successful US test in the mid-1980s, there was no further destructive DA-ASAT test until 2007, when China destroyed one of its own defunct satellites, generating massive amounts of debris in orbit. Only one year after the Chinese test, the USA destroyed one of its own satellites in another debris-generating test, using the Standard Missile 3 (SM-3) Block IIA interceptor that is part of its Aegis sea-based missile defence system.[82] In 2021 Russia also destroyed one of its own defunct satellites, again creating significant debris.[83] The test reportedly used the Nudol interceptor, which Russia is developing as part of the modernization of the strategic missile defence system around Moscow.

All destructive DA-ASAT tests conducted thus far have targeted satellites in LEO. China is possibly at the experimental phase of developing DA-ASAT weapons for higher orbits, based on a 2013 rocket launch. While Chinese media reported this launch as a high-altitude scientific experiment, the US DOD argues that it indicates China's plans to pursue ASAT weapons that target satellites up to GEO.[84] However, given the limited evidence, it is unlikely that this capability is operational.[85]

[79] Grego (note 4), p. 275.

[80] Weeden, B. and Samson, V. (eds), *Global Counterspace Capabilities: An Open Source Assessment 2023* (Secure World Foundation: Broomfield, CO, Apr. 2023), pp. 01-14–15.

[81] Grego, L., 'A history of anti-satellite programs', Union of Concerned Scientists, Jan. 2012.

[82] Grego, L., 'The anti-satellite capability of the Phased Adaptive Approach missile defense system', Public Interest Report, Federation of American Scientists, winter 2011.

[83] Russian Ministry of Defence, 'Russian Defence Minister General of the Army Sergei Shoigu confirms successful test of anti-satellite system', 16 Nov. 2021; and TASS, 'New Russian system being tested hit old satellite with "goldsmith's precision"—Shoigu', 16 Nov. 2021.

[84] China News, [China conducts another high-altitude scientific exploration test: Higher altitude and more data], 14 May 2013 (in Chinese); and US Department of Defense (note 30), p. 93.

[85] Weeden and Samson (note 80), p. 03–16.

Co-orbital anti-satellite weapons

Like DA-ASAT weapons, co-orbital ASAT weapons are kinetic weapons. However, the latter strike their targets from orbit, rather than directly from the ground. To strike, a co-orbital ASAT weapon is launched into space; it can then either stay in orbit undetected or immediately undertake manoeuvres to move towards the target. After it manoeuvres close to the target, the attack is conducted by using either an interceptor or pellets to collide with the target. The term co-orbital ASAT could also refer to a space asset that carries a harpoon or a robotic arm to attack a target satellite.

To manoeuvre a co-orbital ASAT weapon close to its target requires the ability to conduct precise rendezvous and proximity operations (RPOs). RPOs have diverse applications including civilian ones; for instance, RPOs enable servicing and maintenance of satellites and the docking of capsules with the International Space Station. Because of their multiple purposes, an RPO capacity by itself does not necessarily mean that a state has an active co-orbital ASAT capability. For example, a state may conduct an RPO to manoeuvre an inspector satellite close to a rival's satellite and collect intelligence by taking photographs. Nonetheless, RPOs represent a significant technological advance that is a prerequisite for co-orbital ASAT weapons. For this reason, such manoeuvres between the space assets of rival states, particularly without prior notification, can be highly escalatory.

Detailed information on the RPOs of China, Russia and the USA involving their own satellites is limited, and none of the three has publicly acknowledged a co-orbital ASAT capability. However, the Soviet Union's ASAT programme originally focused on development of co-orbital ASAT weapons.[86] Based on this past programme, Russia has the potential to reinvigorate relevant technologies for research, development or testing purposes. Some observers also point to evidence of Russia's development since the early 2010s of new co-orbital ASAT weapons in connection with its space situational awareness (SSA) capabilities.[87]

There is no established minimum distance to be maintained between satellites, nor a requirement for states to notify each other of RPOs. Manoeuvres near another state's satellite without prior communication or notification are sometimes referred to as 'non-consensual' or 'uncoordinated' RPOs. China, Russia and the USA have each conducted such RPOs near other states' satellites in LEO and GEO, with the frequency of such operations increasing over the past decade.[88] These include a number of close approaches in orbit by the USA towards Chinese and Russian satellites, and by Russia towards US satellites. China has reported that US satellites made 14 close approaches to its satellites between 2020 and 2021.[89] Reports also indicate that China has conducted such RPOs near US satellites.[90]

[86] On the origins of the programme see ed. Podvig (note 18), pp. 433–34.

[87] Weeden and Samson (note 80), pp. 02-01–14.

[88] Weeden and Samson (note 80); and Bingen, K. A., Johnson, K. and Young, M., *Space Threat Assessment 2023* (Center for Strategic and International Studies: Washington, DC, Apr. 2023).

[89] Chen, S., 'Study says US spy satellites approaching China's high-value space assets a "threat to security"', *South China Morning Post*, 5 May 2023.

[90] Jones, A., 'A Chinese spacecraft has been checking out US satellites high above earth', Space, 3 Mar. 2023.

Some Chinese researchers have raised concerns about RPOs, particularly in relation to the Starlink satellites owned by SpaceX. These include concerns surrounding Starlink's autonomous 'manoeuvring capability to change orbit'.[91] Other Chinese researchers have expressed concerns regarding potential cyberattacks enabled by RPOs through internet satellite constellations (e.g. Starlink), although there is limited evidence that this is feasible.[92]

Electronic interference

Electronic interference or electronic warfare in space can refer to different types of attacks on space systems through the electromagnetic spectrum. These include jamming (i.e. emission of noise into the frequency to disrupt the signal), spoofing (i.e. creation of a false signal to mislead the receiver) and meaconing (i.e. interception and rebroadcasting of a navigation signal).

Among these, jamming in particular has been increasingly used by states against adversaries' satellites. The difficulty of attribution makes jamming an attractive means of counterspace attack, enabling the aggressor to avoid accountability. Additionally, despite being described as an 'attack', states have not reached a consensus on when electronic interference with space systems constitutes a use of force under international law.[93] Because its effects can be reversible and temporary, jamming lies in a 'grey zone' as hostile behaviour that is intended to remain below the threshold of armed conflict.

State-sourced information on electronic warfare capabilities is highly classified. Expert assessments conclude that China, Russia and the USA all have operational electronic warfare counterspace capabilities, although only Russia and the USA have actively used their capabilities in conflict.[94]

The USA has published details of its Counter Communications System (CCS), which 'reversibly denies adversary satellite communications'.[95] The USA also has the ability to jam GNSS signals—its Joint Navigation Warfare Centre lists one of its tasks as being, 'when directed, [to] prevent effective use of PNT services by adversaries'.[96]

Russia publicly acknowledges having a counterspace capability to jam navigation and communications satellites.[97] The importance of electronic warfare has also been emphasized by Russian military officials.[98] Russia is likely to have a wide range of unacknowledged capabilities for electronic

[91] Ren, Y. et al., [The development status of Starlink and its countermeasures], *Modern Defence Technology*, vol. 50, no. 2 (Apr. 2022), p. 14 (in Chinese; author translation).

[92] Yuan, Y., 'Chinese thinking on the space–cyber nexus', Cybersecurity and Outer Space Essay no. 16, Centre for International Governance Innovation (CIGI), 29 Jan. 2023.

[93] E.g. on the intergovernmental discussion on this issue in relation to the Chinese–Russian draft treaty on prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (PPWT) see Conference on Disarmament, Letter dated 19 August 2008 from the Permanent Representative of the United States of America, CD/1847, 26 Aug. 2008, para. 5(i).

[94] Weeden and Samson (note 80); and Bingen et al. (note 88).

[95] US Space Force, 'Counter Communications System Block 10.2 achieves IOC, ready for the warfighter', 13 Mar. 2020.

[96] US Space Command, 'Joint Navigation Warfare Center', Fact sheet, [n.d.].

[97] Rosoboronexport, 'Reconnaissance and electronic warfare means: R-330ZH', [n.d.].

[98] E.g. see the interview with Colonel Sergei Ivantei in Surovtsev, O., [The craftmanship secrets of the 'gods of war'], *Suvorovskii natisk*, 20 Nov. 2020, p. 3 (in Russian).

warfare that can also jam or spoof satellite signals.[99] Some Russian media reports suggest that it has the capability to jam satellites in GEO, although there is little information about the system and its effectiveness.[100] Russia is also suspected of having jammed GPS in Finland and Norway during a 2018 exercise by the North Atlantic Treaty Organization (NATO).[101] In the war in Ukraine, Russia reportedly tried to jam the Starlink satellites used by the Ukrainian military.[102]

While China does not acknowledge possessing electronic warfare capabilities, multiple incidents of jamming and spoofing have been attributed to China by other states and media sources.[103] US military and intelligence reports also mention China's electronic warfare counterspace capabilities.[104]

Directed-energy weapons

Directed-energy weapons, as the name suggests, direct concentrated energy (in the form of electromagnetic pulses, microwave beams or lasers) to attack space systems. Lasers in particular can interfere with the optical sensors of space systems temporarily by 'dazzling' or permanently by 'blinding'. While lasers could also theoretically have a permanent impact by causing the satellite bus (i.e. the main structure of the satellite) to overheat, it is unclear whether any state has a capability to do so.[105] China, Russia and the USA each appear to be pursuing R&D of directed-energy weapons, particularly lasers, although none acknowledges doing so with the objective of disrupting space systems.

The USA publicly acknowledges having developed a laser counterspace capability in the 1980s, which it tested against a satellite in 1997.[106] This system could be operationalized in the future to attack satellites.[107]

Russia has made several statements claiming that it has lasers that can attack space systems.[108] While some of those claims have been disputed, experts conclude that Russia too has the potential to harness existing R&D and operationalize lasers to attack space systems in the future.[109]

[99] Hendrickx, B., 'Russia gears up for electronic warfare in space (part 1)', Space Review, 26 Oct. 2020; Hendrickx, B., 'Russia gears up for electronic warfare in space (part 2)', Space Review, 2 Nov. 2020; and Weeden and Samson (note 80), pp. 02-22–27.

[100] RIA Novosti, [Russia has developed a new electromagnetic warfare system, said a source], 15 Apr. 2023 (in Russian).

[101] Reuters, 'Norway says it proved Russian GPS interference during NATO exercises', 18 Mar. 2019; and GPS World, 'Norway, Finland suspect Russia of jamming GPS', 12 Nov. 2018.

[102] E.g. Insinna (note 41); and Horton (note 41).

[103] E.g. US Department of Defense (note 30); and EurAsian Times, 'China has deployed "satellite jammers" near Indian border as PLA gets battle-ready at breakneck speed', 21 Nov. 2020.

[104] E.g. US Department of Defense (note 30), p. 68; and US Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community* (ODNI: Washington, DC, 6 Feb. 2023), p. 8.

[105] Wright, D., Grego, L. and Gronlund, L., *The Physics of Space Security: A Reference Manual* (American Academy of Arts and Sciences: Cambridge, MA, May 2005), p. 134.

[106] US Defense Advanced Research Projects Agency (DARPA), 'MIRACL', [n.d.]; and US Department of Defense, 'Secretary of Defense approves laser experiment to improve satellite protection', News release no. 526–97, 2 Oct. 1997.

[107] Weeden and Samson (note 80), pp. 01-27–28.

[108] Hitchens, T., 'Don't be dazzled by Russia's laser weapons claims: Experts', Breaking Defense, 19 May 2022.

[109] Hendrickx, B., 'Peresvet: A Russian mobile laser system to dazzle enemy satellites', Space Review, 15 June 2020.

In contrast to Russia and the USA, there is no state-sourced evidence of China having directed-energy weapons. However, in 2006 the USA claimed that one of its satellites had been 'illuminated' by a ground-based laser operating in China.[110] China did not respond publicly to the allegations.

Based on this limited information, it appears that none of the three states has has operationalized directed-energy weapons to target space systems. If laser capabilities do mature in the future, it is likely that space systems with optical sensors, such as ISR satellites, are most vulnerable to attack by these means.

Cyber

Space systems rely on cyber components for both transmission and storage of data. As a result, cyberattacks constitute a significant threat to space systems that can affect their ground segment, their user segment, or the links between satellites and terrestrial stations. However, it is difficult to ascertain the offensive cyber capabilities of states, let alone any cyber capabilities that can specifically target space systems. Actors in the space domain are not only reluctant to reveal details of the development of their own offensive cyber capabilities, but they are also reluctant to acknowledge having fallen victim to cyberattacks as this would mean acknowledging the vulnerability of their systems.[111] Furthermore, attributing the source of a cyberattack continues to be hard and opens the accountability of the attacking state to dispute.[112]

There are few detailed reports of cyberattacks on space systems.[113] The most recent—which coincided with the Russian invasion of Ukraine on 24 February 2022—involved the user segment of a commercial satellite communications network belonging to Viasat.[114] The attack disrupted services for users across several states in Europe, temporarily disrupted services for the Ukrainian military, affected emergency services in France and knocked offline over 5000 wind turbines in Germany. Several states, including the USA, attributed the cyberattack to Russia, although Russia did not publicly claim responsibility.[115]

Despite limited information on cyber capabilities, the Viasat case shows how space systems are becoming increasingly appealing targets for cyberattacks. Chinese experts have raised specific concerns regarding cyberattacks against space systems for navigation, early-warning and communications functions, with one stating that such attacks 'will lead to an unintended escalation of conflict'.[116] Accordingly, some observers caution against a focus on the governance of 'flashier kinetic counterspace threats' while cyber counterspace capabilities are overlooked.[117]

[110] SpaceNews, 'NRO confirms Chinese laser test illuminated US spacecraft', 3 Oct. 2006.

[111] Samson, V., 'The cyber counterspace threat: Coming out of the shadows', Cybersecurity and Outer Space Essay no. 7, Centre for International Governance Innovation (CIGI), 29 Jan. 2023.

[112] E.g. Kastelic, A., *Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics* (UNIDIR: Geneva, Jan. 2022).

[113] Weeden and Samson (note 80); and Bingen et al. (note 88).

[114] Raju and Saalman (note 43), pp. 489–90.

[115] Blinken, A. J., US Secretary of State, 'Attribution of Russia's malicious cyber activity against Ukraine', Press statement, US Department of State, 10 May 2022.

[116] Yuan (note 92).

[117] Samson (note 111).

Space situational awareness

Space situational awareness (sometimes referred to as space domain awareness) refers to the tracking and identification of space objects. This includes monitoring and predicting the movements of satellites and debris. The usefulness of SSA for a future international space traffic management system has been demonstrated by its ability to warn of potential collisions in orbit. At the same time, however, SSA is still considered a counterspace capability as it is critical to identification of a target space system.

SSA consists of a network of radars and sensors, which can be both terrestrial and space based. At present, states rely more on terrestrial sensors while they pursue development of space-based sources. The technology for SSA radars is derived from Soviet and US early-warning systems, which is why Russia and the USA currently have the most advanced SSA capabilities. Even today, the USA uses the same ground-based radars for detection of missile launches and for conducting space surveillance and tracking.[118] Chinese experts have highlighted the need to enhance China's SSA capabilities.[119] Nevertheless, the US DOD estimates that China has a robust space-surveillance network including sensors, telescopes and radars.[120]

IV. Assessing vulnerabilities

As noted above, China, Russia and the United States each use space systems for various nuclear deterrence-related functions, and each also possesses counterspace capabilities by which it can hold the others' space systems under threat. On the basis of the preceding sections, this section assesses vulnerabilities of existing space systems to attack or disruption by counterspace capabilities. A system's vulnerability to counterspace capabilities varies depending on the type of system and the orbit into which it is launched. Perceived or actual exploitation of such vulnerabilities could have a significant impact on strategic stability among the three states, notably by contributing to the risk of nuclear escalation.

Early-warning satellites and strategic communications satellites

Current early-warning satellites (which are used to detect incoming missiles) and strategic communications satellites (which relay messages within a state's nuclear command chain) are in GEO and HEO. Based on the known counterspace capabilities of China, Russia and the USA, these satellites are vulnerable to attack primarily through co-orbital, electronic or cyber means.

Existing DA-ASAT capabilities cannot reach GEO, while using DA-ASAT weapons against satellites in HEO, even at their lowest point, would be challenging given the satellites' high speed and the limited window for interception. Thus, satellites in lower orbits presently remain most vulnerable to DA-ASAT weapons. However, as the USA's plans for disaggregation suggest, early-warning systems might diversify in the coming decades to

[118] E.g. US Space Force, 'PAVE PAWS Radar', Fact sheet, Oct. 2020; and US Air Force Space Command, 'Perimeter Acquisition Radar Attack Characterization system', Fact sheet, 2 Mar. 2017.
[119] Ren (note 91).
[120] US Department of Defense (note 28), p. 92.

include satellites in LEO and MEO.[121] Given previous cases of interference with satellites in LEO and MEO, this change could increase the vulnerability to DA-ASAT weapons of space-based components of early-warning systems.

Given the significance of early-warning and strategic communications satellites for NC3, any attack on them would be extremely escalatory. If the targeted state were to interpret such an attack as preparation for a nuclear first strike, it could decide to launch a second strike. Even though the decision to retaliate would probably also require confirmation of an attack by radar, the limited response time—particularly in countries such as Russia and the USA with a launch-on-warning nuclear posture—might lead to fatal consequences. While an intentional attack on an early-warning or strategic communications satellite therefore seems unthinkable except within the context of an imminent or ongoing nuclear war, such an attack could still take place as a result of leaders' misjudgement. This could stem from increasing entanglement of nuclear and non-nuclear capabilities, related to the multifunctional nature of some of these satellites. For example, some observers have highlighted the risk that US early-warning satellites could be targeted in a regional conflict in order to undermine theatre missile defences; while intended to undermine the non-nuclear capabilities of the USA or its allies, the USA could regard such an attack as targeting its nuclear capabilities and respond accordingly.[122] There is also considerable scope for misperceptions and miscalculation; in addition to the possibility of false attribution of a non-kinetic attack or a non-consensual RPO, technical deficiencies or malfunctions in an early-warning system could lead to false alarms.

Intelligence, surveillance and reconnaissance satellites and other communications satellites

ISR satellites, located in both GEO and LEO, provide information on adversaries' nuclear weapon infrastructure and relevant activities, thus facilitating counterforce targeting and offering clues of potential changes in deployment practices and alert levels. The role of ISR satellites in LEO is growing as China, Russia and the USA each seek to enhance their space-based surveillance capabilities. This development has been partly prompted by the perceived need for detection of and response to the emerging threat of hypersonic missiles. In addition to strategic communications satellites in GEO, other communications satellites are also increasingly being launched into LEO. These include megaconstellations such as Starlink that can serve various military needs.

Disruption or interference using non-kinetic capabilities, for instance electronic or cyber operations, are likely against ISR and communications satellites in LEO. As noted in section III, such incidents have already taken place.[123] In principle, ISR and communications satellites in LEO are also vulnerable to attack by DA-ASAT and co-orbital ASAT weapons. However, the space debris created by a kinetic strike would drastically pollute the

[121] Hitchens (note 11).

[122] Zhao, T. and Bin, L., 'The underappreciated risks of entanglement: A Chinese perspective', ed. Acton (note 2), p. 51.

[123] Insinna (note 41); Horton (note 41); and Raju and Saalman (note 43), pp. 489–90.

whole orbit, with an impact also on the attacking state. Given that China, Russia and the USA each depend on LEO for military and civilian needs, the indiscriminate effects of space debris would create a lose–lose situation for the attacking and targeted states, and also for all other users of LEO including the attacker's allies.

Attacks on such ISR and communications satellites could involve various escalation risks, depending on the context. As noted above, targeting multifunction satellites used for both ISR and early-warning purposes in GEO would involve a high risk of nuclear escalation. While the risks may be lower in case of an attack on an ISR or communications satellite in LEO, any use of counterspace capability—whether using an ASAT weapon or temporary or reversible interference—would still create tensions and contribute to general escalation during a crisis. Current US plans for the deployment of multifunction early-warning and ISR satellites in LEO to track hypersonic weapons could also involve new nuclear escalation risks as the threshold for attacking them might be lower than for early-warning satellites in GEO.

Navigation satellites

Navigation satellites for GNSS are integral to the advanced military capabilities of China, Russia and the USA as they facilitate the tracking, targeting and guidance of missiles and other weapons to their targets. Together with ISR and communications satellites, GNSS therefore enables precision-strike weapons. In addition, some Russian and US navigation satellites are also used to detect nuclear detonations. While GNSS may also be used as part of the guidance systems of some nuclear weapons, states likely prefer additional means of navigation for this purpose because GNSS can be vulnerable to interference, such as jamming.

China, Russia and the USA each have advanced electronic and cyber counterspace capabilities that can interfere with GNSS, and both Russia and the USA have employed jamming and spoofing against their adversaries' GNSS signals.[124] Due to the difficulty of attributing such interference, this grey zone activity is relatively frequent, and it appears to be increasingly considered a tool of modern warfare by all three states. In contrast, a kinetic attack on a GNSS satellite would be unprecedented and, due to the resulting debris (which would also undermine the attacking state's own warfighting capability), counterproductive.

V. Conclusions

Space systems are critical to the nuclear deterrence practices of China, Russia and the United States, although the extent to which they have integrated these systems into these practices varies. Space assets in GEO and HEO have long been a crucial part of the early-warning systems of the USA and, to a relatively lesser extent, Russia. In contrast, China seems to be in the early stages of building up its space-based early-warning system. Each of the three states also uses satellites for strategic communications, which in the Russian and US cases includes the transmission of orders to launch nuclear

[124] Weeden and Samson (note 80); and Bingen et al. (note 88).

weapons. In addition, China, Russia and the USA all have ISR, navigation and communications satellites that can facilitate nuclear counterforce targeting as well as high-precision strikes, including potential strikes with nuclear-capable ballistic missiles, hypersonic weapons and guided bombs.

At the same time, each of the three states possesses advanced counterspace capabilities. Development of these capabilities has accelerated in recent years, reflecting the increased importance of space systems in modern warfare. Destructive tests of DA-ASAT weapons represent the most visible demonstration of this trend, although their use would be counterproductive for any country that relies on satellites for civilian or military uses. Non-kinetic means of disrupting ISR and communications satellites in LEO and navigation satellites in MEO have already been used and can be expected to be used in the future, particularly in connection with regional conflicts.

Given the importance to NC3 of early-warning and strategic communications satellites in GEO and HEO—and the consequent high risk of escalation if they were to be attacked—such satellites are unlikely targets. But this will remain true only so long as leaders are deterred by the prospect of nuclear war. Thus, direct nuclear escalation resulting from a space-enabled attack against a rival's most sensitive space systems in GEO and HEO cannot be ruled out.

In addition to the risk of inadvertent escalation, particularly in connection with non-consensual or uncoordinated RPOs between rivals, there is also the possibility that a technical malfunction will be misinterpreted as a hostile act. Similarly there is potential for false attribution of acts of sabotage by a third party. The continued advances in counterspace capabilities coupled with a lack of clear legal and normative regulations arguably add to the risk of such inadvertent escalation. Attacks on or interference with satellites in LEO and MEO—even non-kinetic attacks—further contribute to tensions and potential escalatory spirals among nuclear-armed states.

Overall, these developments point to the need to put space systems at the centre of the study of nuclear escalation pathways and include them in proposals for future risk-reduction measures.

Abbreviations

ABM	Anti-Ballistic Missile (Systems Treaty)
AI	Artificial intelligence
ASAT	Anti-satellite (weapon)
DA-ASAT	Direct-ascent anti-satellite (weapon)
DOD	Department of Defense (United States)
GEO	Geostationary orbit
GLONASS	Global Navigation Satellite System (Russia)
GNSS	Global navigation satellite system
GPS	Global Positioning System (United States)
HBTSS	Hypersonic and Ballistic Tracking Space Sensor (United States)
HEO	Highly elliptical orbit
ICBM	Intercontinental ballistic missile
IMINT	Imagery intelligence
ISR	Intelligence, surveillance and reconnaissance
LEO	Low earth orbit
MEO	Medium earth orbit
NC3	Nuclear command, control and communications
PNT	Position, navigation and timing
R&D	Research and development
RPO	Rendezvous and proximity operation
SAR	Synthetic-aperture radar
Satcom	Satellite communications
SBIRS	Space-Based Infrared System (United States)
SIGINT	Signals intelligence
SSA	Space situational awareness

RECENT SIPRI PUBLICATIONS

Cyber Crossover and Its Escalatory Risks for Europe
Lora Saalman, Fei Su and Larisa Saveleva Dovgal
SIPRI Insights on Peace and Security
September 2023

The Arctic is Hot: Addressing the Social and Environmental Implications
Emilie Broek
SIPRI Policy Brief
September 2023

Integrating Gender Perspectives into International Humanitarian Law
Nivedita Raju and Laura Bruun
SIPRI Insights on Peace and Security
August 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Measurement
Marie Riquier
SIPRI Report
June 2023

Russia's Military Expenditure During Its War Against Ukraine
Professor Julian Cooper
SIPRI Insights on Peace and Security
June 2023

The Role of Umbrella States in the Global Nuclear Order
Dr Tytti Erästö
SIPRI Insights on Peace and Security
June 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Stabilization
Dr Caroline Delgado
SIPRI Report
May 2023

The World Food Programme's Contribution to Improving the Prospects for Peace in Sri Lanka
Dr Simone Bunse and Dr Vongai Murugani
SIPRI Report
May 2023

Comparing Responses to Climate-related Security Risks Among the EU, NATO and the OSCE
Anniek Barnhoorn
SIPRI Policy Report
April 2023

SIPRI BACKGROUND PAPER

THE ROLE OF SPACE SYSTEMS IN NUCLEAR DETERRENCE

NIVEDITA RAJU AND TYTTI ERÄSTÖ

CONTENTS

I.	Introduction	1
II.	Space systems relevant to nuclear deterrence	2
	Missile early warning	3
	Communications	7
	Intelligence, surveillance and reconnaissance	8
	Navigation	10
III.	Counterspace capabilities	12
	Direct-ascent anti-satellite weapons	13
	Co-orbital anti-satellite weapons	14
	Electronic interference	15
	Directed-energy weapons	16
	Cyber	17
	Space situational awareness	18
IV.	Assessing vulnerabilities	18
	Early-warning satellites and strategic communications satellites	18
	Intelligence, surveillance and reconnaissance satellites and other communications satellites	19
	Navigation satellites	20
V.	Conclusions	20
	Abbreviations	22
	Box 1. Types of orbit	4
	Figure 1. Types of satellite	2

ABOUT THE AUTHORS

Nivedita Raju (India) is a Researcher in the SIPRI Weapons of Mass Destruction Programme. Her recent research focuses on trends in space security, space governance and transparency and confidence-building measures.

Dr Tytti Erästö (Finland) is a Senior Researcher in the SIPRI Weapons of Mass Destruction Programme, focusing on nuclear disarmament and non-proliferation issues.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org