sipri

SIPRI Research Policy Paper

February 2025

PARAMETERS TO ASSESS ESCALATION RISKS IN SPACE

NIVEDITA RAJU*

SUMMARY

● Space-enabled services are critical for various civilian and military purposes. Current military uses of space—for example, in the Russia–Ukraine War—indicate several avenues for unpredictability and ambiguity, which can increase potential for escalation, both in space and on earth. Yet, there is no common understanding of escalation risks in the international community.

This SIPRI Research Policy Paper identifies four parameters to assess escalation risks in the space domain: the target, the capability used, the effect and the consequences. These parameters can help establish a standardized approach to assess whether an attack is escalatory.

Based on current trends that undermine predictability and transparency in space activities, these parameters inform recommendations to minimize escalation risks. These recommendations include proposals to limit attacks on high-value strategically significant space systems; undertake exchanges on critical infrastructure; characterize acts that are especially escalatory; to enhance resilience of space-based services for civilians; and to build a typology that identifies potential harms. The recommendations also demand further action from states to implement and enforce international law governing space activities and to engage with commercial actors to raise awareness and clearly establish their accountability.

Technological advances in outer space, in cyberspace and in artificial intelligence (AI) have changed how states conduct military operations. These technologies, and space systems in particular, can offer decisive military benefits by enabling weapon systems, both nuclear and non-nuclear.[1] Moreover, the surge of the commercial space sector means that the types of actors now engaged in space activities differ from those of the cold war.[2] In parallel, numerous actors have gained and strengthened their abilities to target space systems.

These developments have influenced states' threat perceptions, have heightened strategic rivalries and, in some cases, have even accelerated arms-racing behaviours. Such dynamics are prominent in Europe amid the changing security environment following the Russian Federation's full-scale invasion of Ukraine in February 2022. Russia's emphasis on the deterrent role of nuclear weapons along with military use of space by both parties in the conflict have raised concerns about escalation, possibly even to nuclear use. This does not mean that all threats to or attacks on space systems will necessarily lead to the use of nuclear weapons. However, there is scope for perceived threats to fuel escalation across domains, especially inadvertent escalation driven by uncertainties, misperceptions and miscalculations in outer space. This highlights the need for common understandings on escalation risks in the space domain.

This SIPRI Research Policy Paper aims to provide a foundation for such common understandings on escalation risks by identifying parameters to assess actions that states perceive as being escalatory in the space domain. It first outlines (in section I) current military uses of space, drawing examples from the Russia–Ukraine War, and examines (in section II) how these trends contribute to unpredictability and ambiguity. It then identifies (in section III) four parameters to define actions that states might perceive as more or less escalatory. These parameters are then used to propose (in section IV) recommendations to reduce risk of escalation before the paper concludes (in section V).

[1] Raju, N. and Erästö, T., 'The role of space systems in nuclear deterrence', SIPRI Background Paper, Sep. 2023.

[2] Brockmann, K. and Heau, L., *The Expansion of the NewSpace Industry and Missile Proliferation Risks* (SIPRI: Stockholm, Oct. 2024).

* The author would like to thank the Foreign, Commonwealth and Development Office of the United Kingdom for its generous funding of this paper.

I. Current military uses of space: Snapshot from Ukraine

The role of space for military purposes is striking in the ongoing war in Ukraine. Unlike Russia, Ukraine is not a traditional 'space power' with its own capabilities. Yet, it has successfully adapted its command structures to utilize its partners' space systems, most prominently those provided by the United States and by US companies. The expansive presence of commercial actors in operations and the extent to which their services have benefitted Ukraine exhibit a shift from earlier uses of space in conflict.

Space systems as critical enablers

By facilitating coordination and dissemination of information among troops, space systems can enhance military operations and logistics. For example, Ukraine has benefitted in this way from the use of Starlink, a constellation of communications satellites provided by SpaceX, a US company. Starlink can effectively relay feeds from uncrewed vehicles to Ukrainian artillery batteries in real time, resulting in greater precision in targeting.[3] Ukrainian troops also reportedly use Starlink to contact US forces for remote technical assistance to fix, maintain and replace weapon systems.[4]

Some of these space systems also provide strategically relevant functions. Satellite communications have enabled Ukrainian President Volodymyr Zelensky to broadcast speeches to national and international audiences, as well as to securely connect to US officials. In addition, satellite imagery allows Ukraine to monitor Russian forces. This has several purposes: it allows Ukrainian troops to identify build-up of Russian forces, to conduct accurate strikes, to use arms efficiently and to conduct battle-damage assessments.[5] Satellite imagery also helps to identify the extent of civilian damage, to document war crimes and to combat disinformation. Such imagery has been used by Ukraine and other actors to raise awareness and muster support, including in multilateral forums when discussing war crimes committed by Russia.[6]

Growing military uses of space in cooperative security arrangements

Military uses of space have increasingly featured in cooperative security arrangements. For example, the North Atlantic Treaty Organization (NATO) relies on space assets of individual members and has been taking steps to streamline its approach. In 2019 it adopted an overarching space policy and declared outer space an operational domain.[7] NATO's 2022 strategic concept expressly recognizes the importance of space for deterrence and defence.[8] It has announced that a commercial space strategy will be issued in 2025.[9]

[3] Dickey, R. and Gleason, M. P., 'Space and war in Ukraine: Beyond the satellites', *Æther*, vol. 3, no. 1 (spring 2024), p. 27.

[4] Tucker, P., 'US soldiers provide telemaintenance as Ukrainians MacGyver their weapons', Defense One, 18 Sep. 2022.

[5] Dickey and Gleason (note 3), p. 29.

[6] E.g. United Nations, General Assembly and Security Council, Letter from the permanent representative of Ukraine to the secretary-general, A/78/857-S/2024/331, 24 Apr. 2024, pp. 2–3.

[7] NATO, 'NATO's overarching space policy', 27 June 2019.

[8] NATO, 'NATO 2022 strategic concept', 29 June 2022.

[9] NATO, 'NATO explores ways to better protect commercial partners in space', 4 Oct. 2024.

There has been a simultaneous shift in the approach of the European Union (EU) to space. EU space applications primarily had a civilian focus but are now being adapted for more defence-oriented missions, as outlined in the EU's 2023 space strategy for security and defence.[10] The strategy also mentions that the EU will conduct space exercises and enhance cooperation with NATO. The EU does not have a dedicated unit for military space operations, nor does it have its own counterspace capabilities. However, individual EU member states, such as France, have expressed interest in counterspace capabilities, particularly directed-energy weapons.[11]

Ukraine has received much of its space support from Western states, with the USA topping its list of suppliers.[12] The USA has equipped Ukraine (referred to as a 'key regional strategic partner') with satellite communications antennas, terminals, electronic warfare and counter-electronic warfare equipment and has also provided commercial satellite imagery services.[13] The USA's Global Positioning System (GPS) is especially important for Ukraine given that the volume of major arms transferred to Ukraine is mostly comprised of missiles, many of which use GPS for navigation.[14]

Meanwhile, there are indications of cooperation between Russia and other states. Belarus and Russia have deepened cooperation on space, aiming to implement a project for a Belarusian remote-sensing space system. This suggests a focus on intelligence, surveillance and reconnaissance (ISR) to, among other objectives, 'improve the effectiveness of accomplishing tasks relating to ensuring national security'.[15] China and Russia are enhancing cooperation for space applications, including monitoring of space debris and navigation services.[16] Cooperation on space is also expressly mentioned in the 2024 strategic partnership treaty between the Democratic People's Republic of Korea (DPRK, or North Korea) and Russia.[17] Russia has additionally supported the Iranian space sector by launching Iranian satellites on Russian rockets.[18]

Rise in cyberattacks and electronic warfare

Given the benefits that space systems provide, including for military uses, there has been a subsequent rise in means to attack them. There are several different ways of attacking or interfering with space systems. These can be

[10] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'European Union space strategy for security and defence', Joint Communication to the European Parliament and the Council, JOIN(2023)9, 10 Mar. 2023.

[11] Pasco, X. and Wohrer, P., 'Implementing the French Space Defence Strategy: Towards space control?', Note no. 15/23, Fondation pour la Recherche Stratégique (FRS), 30 June 2023.

[12] Wezeman, S. T. et al., 'Global trends in arms transfers 2019–23', *SIPRI Yearbook 2024: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2024), p. 239.

[13] US State Department, Bureau of Political-Military Affairs, 'U.S. security cooperation with Ukraine', Fact sheet, 9 Jan. 2025.

[14] Raju and Erästö (note 1), pp. 10–11.

[15] President of Belarus, 'Decree on new Belarusian–Russian space exploration project signed', 15 Apr. 2024.

[16] BeiDou Navigation Satellite System, 'Agreement on China–Russia intergovernmental cooperation on satellite navigation of [*sic*] signed in Beijing', 7 Nov. 2018; and China National Space Administration (CNSA), 'CNSA and ROSCOSMOS have signed agreement on cooperation on space debris monitoring and practical use of gathered data', 26 Nov. 2018.

[17] Korea Central News Agency (KCNA), 'DPRK–Russia Treaty on Comprehensive Strategic Partnership', 20 June 2024.

[18] 'Russian rocket takes Iranian satellites into orbit as ties grow closer', Al Jazeera, 5 Nov. 2024.

classified as kinetic or non-kinetic, based on whether they rely on motion to physically destroy the target. While some actors have kinetic capabilities, no state has ever employed them against another state's space system.

The war in Ukraine exhibits a surge in the number of non-kinetic attacks—cyberattacks and electronic warfare—on space systems. Prominent among these was the February 2022 cyberattack on the Viasat satellite network, which several states attributed to Russia. This cyberattack affected the space system's users across several states in the region, including the Ukrainian military.[19] Some experts have reported cyberattacks conducted by both Russian and Ukrainian actors, including hacker groups that targeted government organizations in each state's space sectors.[20] Elon Musk, the founder of SpaceX, has additionally stated that Russia has conducted cyberattacks against Starlink to undermine Ukrainian forces, with subsequent reports suggesting that Starlink was adept at withstanding Russian interference.[21]

Electronic warfare techniques can be used to interfere with space systems, particularly through jamming and spoofing of global navigation satellite systems (GNSSs), including GPS. Since the full-scale invasion of Ukraine, incidents of electronic warfare have risen in line with cyberattacks. Some of these incidents have even affected neighbouring states that are not party to the conflict. For example, in 2024 there were reports of jamming in Estonia, resulting in closure of civilian aircraft routes that required GPS for navigation.[22] Several other states, including Finland, Norway, Poland and Sweden, have reportedly experienced similar effects, including electronic interference that disrupted air traffic, which experts attribute to Russia.[23]

These attacks indicate a marked difference between the use of space in the Russia–Ukraine War and in previous conflicts. For example, while space systems were a key enabler in the 1990–91 Gulf War, the war in Ukraine marks the first time that both parties in an armed conflict have the means to attack space systems.[24] It is also the first instance where a party to a conflict—Russia—has made explicit threats against such space systems in a multilateral forum.[25] It is unclear from these threats if Russia has considered a kinetic strike on space systems.

[19] Raju, N. and Saalman, L., 'Space attacks and cyberattacks in Ukraine', *SIPRI Yearbook 2023: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2023).

[20] Poirier, C., *Hacking the Cosmos: Cyber Operations against the Space Sector—A Case Study from the War in Ukraine* (ETH Zurich, Center for Security Studies: Oct. 2024); and Saalman, L., Dovgal, L. S. and Su, F., 'Mapping cyber-related missile and satellite incidents and confidence-building measures', SIPRI Insights on Peace and Security no. 2023/10, Nov. 2023.

[21] Howell, E., 'Elon Musk says Russia is ramping up cyberattacks on SpaceX's Starlink systems in Ukraine', Space.com, 14 Oct. 2024.

[22] Ringström, A. et al., 'Finnair pauses some Estonia flights due to GPS interference', Reuters, 29 Apr. 2024.

[23] Grynszpan, E. and Pietralunga, C., 'Russia's GPS jamming intensifies over the Baltic Sea', *Le Monde*, 2 May 2024; and Goward, D., 'As Baltics see spike in NATO jamming, NATO must respond', Breaking Defense, 31 Jan. 2024.

[24] Pike, J., Lang, S. and Stambler, E., 'Military use of outer space', *SIPRI Yearbook 1992: World Armaments and Disarmament* (Oxford University Press: Oxford, 1992), pp. 122–26.

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

II. Trends that undermine predictability in space activities

Overall, the developments described in section II imply several avenues for further unpredictability and ambiguity in space activities. These, in turn, enhance the scope for misperceptions. Misperceptions—particularly incorrect assumptions about states' postures, capabilities and conduct—can alter state relations, intensify military competition and further incentivize arms-racing behaviours. Unpredictability also narrows scope for communication, leaving little room to clarify misperceptions in times of crisis or conflict. Unpredictability additionally feeds mistrust between competing states or rivals and can lead to miscalculations, which subsequently magnifies risk of escalation.

Imbalance in military space capabilities and strategies

Today, multiple actors have different types of counterspace capabilities with which to attack or threaten space systems. A space system is comprised of several components: the ground segment (e.g. receivers and satellite dishes), the space segment (the satellite in orbit and launch vehicle), and data links that connect the ground and space segments and transmit services to users. Each of these components is vulnerable to attack in different ways by different types of counterspace capabilities. These differences highlight the distinct imbalance in space capabilities and strategies of different states.[26] These differences consequently drive unpredictability by stoking fears about unknown responses to attacks on space systems.

Unpredictability can be further exacerbated by unclear regulation of counterspace capabilities under international law, particularly cyberattacks and electronic warfare. Some experts argue that 'fear of the unknown response' may increase reluctance to attack important space systems, similar to the nuclear domain.[27] Yet such fear can simultaneously instigate misperceptions and worst-case scenario assumptions about an adversary.

The war in Ukraine exhibits imbalance in capabilities as Russia has considerable counterspace capabilities. As well as non-kinetic means of attacking space systems, Russia demonstrated its kinetic means most recently in 2021 (against one of its own satellites).[28] In addition, in February 2024 the USA reported that Russia is developing a nuclear anti-satellite capability in orbit.[29] While there are few details of the capability, the reports nevertheless underscore that counterspace capabilities range widely and are not evenly distributed among actors, heightening unpredictability in the ways in which space systems can be attacked and how to respond.

[26] Weeden, B. and Samson, V. (eds), *Global Counterspace Capabilities: An Open Source Assessment* (Secure World Foundation: Broomfield, CO, Apr. 2024); and Swope C. et al., *Space Threat Assessment 2024* (Center for Strategic and International Studies: Washington, DC, Apr. 2024).

[27] Bowen, B. E., 'How to approach NATO deterrence and defence aspects', eds N. Fasolo et al., *Space: Exploring NATO's Final Frontier* (NATO Allied Command Transformation: Norfolk, VA, 2024), p. 87.

[28] Raju, N., 'Russia's anti-satellite test should lead to a multilateral ban', SIPRI, 7 Dec. 2021.

[29] The White House, Press briefing, 15 Feb. 2024; and Stewart, M., 'The nuclear option: Deciphering Russia's new space threat', Interview, Center for Strategic and International Studies (CSIS), 3 May 2024.

Influence of private sector actors

Actors in the private sector can undermine predictability in space activities in several ways.

First, the incentive structures for a state, for a company and for individuals differ. For example, while the USA as a state is motivated by security considerations in its support for Ukraine, SpaceX is a company motivated by profit. These interests can converge—after SpaceX initially provided Starlink to Ukraine, by June 2023 the US Department of Defense had agreed to pay for provision of these services to Ukraine.[30] But a company may change its decision to provide services to a party in a conflict, depending on its financial projections and on the personal views of its management. This contributes to unpredictability because it is unclear how long and under what circumstances a party to a conflict has access to that company's services. This possibility became clear in February 2023 when Gwynne Shotwell, president of SpaceX, announced that the company would terminate the Starlink services that enabled uncrewed vehicles for the Ukrainian military, claiming that '[Starlink] was never intended to be weaponized'.[31] No further announcements followed this statement and Starlink continued to be provided to Ukraine. Yet the episode highlights how the private sector has considerable decision-making power in granting or denying major military advantage to a party in an armed conflict. In another example, in September 2023 Musk publicly stated that SpaceX had rejected a request from Ukraine 'to activate Starlink all the way to Sevastopol' as this would have made SpaceX 'explicitly complicit in a major act of war and conflict escalation'.[32]

Second, the public-facing persona of individuals such as Musk can also contribute to unpredictability. If Musk gains formal political authority in the new administration of US President Donald J. Trump, his public statements may inflame misperceptions about whether his views are personal or reflect official US policy. These include questions about whether Musk would deny Taiwan access to Starlink services in case of a future conflict with China.[33]

Third, companies can magnify uncertainty from a regulatory standpoint. There is no consensus on how a company's engagement in conflict has an impact on neutral states under international law, nor is there clarity on how such a company can be held accountable for its actions in a conflict. This is particularly the case if a party to a conflict gains unauthorized access to commercial space services. For instance, in 2024 a Ukrainian military official claimed that Russian forces had illicitly obtained and were using Starlink terminals (which are small and easily portable).[34] Musk stated that, 'To the best of our knowledge, no Starlinks have been sold directly or indirectly to Russia.'[35] These reports triggered inquiries within the USA about private

[30] Stone, M. and Roulette, J., 'SpaceX's Starlink wins Pentagon contract for satellite services to Ukraine', Reuters, 1 June 2023.

[31] Foust, J., 'Shotwell: Ukraine "weaponized" Starlink in war against Russia', *Space News*, 8 Feb. 2023.

[32] Musk, E. (@elonmusk), X.com, 8 Sep. 2023.

[33] Davidson, H., 'Anger in Taiwan over reports SpaceX asked suppliers to move abroad', *The Guardian*, 7 Nov. 2024.

[34] Peleschuk, D. et al., 'Russia is using Starlink in occupied areas, Ukraine says', Reuters, 11 Feb. 2024.

[35] Peleschuk et al. (note 34).

sector accountability, specifically SpaceX's obligation to identify and terminate illicit use by Russian forces since it undermined Ukraine's defence.[36]

Potential impacts on civilians

There is an absence of international consensus on the types of risk to civilians that stem from threats to space systems, as well as measures to minimize them. This contributes to unpredictability because it is unclear how a state would respond if an attack on a space system were to have a severe impact on its civilians. The frequency of non-kinetic attacks coupled with a lack of state action suggests that a party to a conflict may be willing to conduct such attacks if it believes they are normalized and permissible, and if it believes they are necessary to disrupt dual-use (i.e. military and civilian) space systems for military advantage. However, even non-kinetic attacks can have devastating consequences and can violate international law if they affect essential services for civilians.

There can be different types of risk to civilians and varying potential consequences depending on the scenario. The International Committee of the Red Cross (ICRC) has reminded states that the supply of humanitarian aid depends on space systems and has provided examples where aid workers are dependent on the imagery, communications and navigation functions of space systems for their daily work.[37] For instance, humanitarian workers depend on GNSSs such as GPS for logistics planning, identifying safe passage routes for civilians in conflict zones and delivering emergency relief supplies.[38] Despite the risks to civilians, states have neither exchanged views on how they consider these risks when using space for military purposes nor have they discussed critical infrastructure in multilateral forums on space security.[39]

Diverging views among states, including allies

While military uses of space are increasingly prominent in partnerships and security alliances, there is no common understanding among these states—even like-minded ones—on escalation risks. This contributes to unpredictability because states do not share the same risk calculus and have no agreement on escalation thresholds, or lawful and proportional responses to attacks. This was most recently demonstrated in May 2024, when Ukraine conducted two uncrewed vehicle attacks against missile early-warning radars that form an element of Russia's nuclear deterrent.[40] This appears to have raised major concerns in the USA, prompting US officials to caution

[36] Office of US Senator Elizabeth Warren, 'At hearing, Warren presses DoD officials to hold SpaceX accountable for Russia's illegal use of Starlink services', Press release, 21 May 2024.

[37] United Nations, General Assembly, Open-ended Working Group on Reducing Space Threats, 'Preliminary recommendations on possible norms, rules and principles of responsible behaviours relating to threats by states to space systems', Working paper submitted by the International Committee of the Red Cross (ICRC), A/AC.294/2023/WP.7, 31 Jan. 2023.

[38] Doucet, G. and Eves, S., *Protecting Essential Civilian Services on Earth from Disruptions by Military Space Operations* (International Committee of the Red Cross: Geneva, June 2024).

[39] Raju, N., 'Space security governance: Steps to limit the human cost of military space operations', Humanitarian Law and Policy, International Committee of the Red Cross (ICRC), 22 Aug. 2023.

[40] Liang, X., 'Ukraine strikes Russian early-warning radars', *Arms Control Today*, vol. 54, no. 6 (July/Aug. 2024).

their counterparts in Ukraine.[41] These diverging views—which can further heighten unpredictability—are equally prominent in the context of threats to or attacks on space systems.

Lack of consensus on escalation thresholds can be compounded by strategic ambiguity in doctrines. For example, in September 2024 Russia announced a new 'red line' at which it would consider using nuclear weapons: if Ukraine were to conduct long-range strikes into Russian territory with weapons supplied by Western states.[42] Russia implied that it would consider NATO members as becoming parties to the conflict, noting that the targeting of the supplied weapons is enabled by Western space systems.[43] This was followed by changes in Russian nuclear doctrine.[44] Ukraine is neither a nuclear-armed state nor a member of NATO; however, Russia's nuclear doctrine suggests that, in response to an attack on its early-warning infrastructure (which includes radar and early-warning satellites), it could possibly use nuclear weapons. Should Russia perceive its nuclear command, control and communications (NC3) system to be threatened, there is substantial scope for escalation, even to nuclear use.[45]

III. Parameters to assess escalation risks

The previous sections outline military uses of space and implications of current trends for further unpredictability. However, there is no clear means to assess how these developments could affect escalation dynamics. This section therefore proposes a framework of four parameters to identify conditions in which an attack on a space system could lead to escalation, while accounting for these developments in a systematic manner. These parameters are (*a*) the target of the attack; (*b*) the capability used in the attack; (*c*) the effect of the attack; and (*d*) its consequences. Consideration of these parameters can in turn inform the design of measures to reduce risk of escalation.

This framework of initial parameters can be applied and adapted to specific contexts. The predominant characteristic of risk is that it is versatile and highly context dependent—for example, parameters can identify potential for escalation, but the likelihood that escalation would actually take place differs depending on contextual variables. These can include the actors involved, the security environment, the presence of security alliances or partnerships, and the overarching political context (e.g. whether there is an active conflict, crisis, flashpoint or deteriorating relations). The following parameters are thus a useful starting point and provide a baseline for assessing actions in the space domain that states might perceive as more or less escalatory. This helps provide a foundation for common understandings on escalation risk among all users of space.

[41] Liang (note 40).
[42] Rosenberg, S., 'Putin draws new red line on long-range missiles', BBC, 13 Sep. 2024.
[43] Rosenberg (note 42).
[44] President of Russia, 'Executive order approving the basic principles of state policy of the Russian Federation on nuclear deterrence', 19 Nov. 2024; and Russian Presidential Decree no. 991 'On approval of the basic principles of the state policy of the Russian Federation on nuclear deterrence', 19 Nov. 2024 (in Russian).
[45] Russian Presidential Decree no. 991 (note 44), para. 19.

Parameter 1. The target

States have varying dependencies on, functions in and uses of space for military and civilian purposes. The value and strategic significance of space systems therefore differ. Consequently, responses to an attack on high-value or strategically significant systems will be more severe.

An attack by any capability on NC3 systems would be extremely escalatory as it may be construed as a direct attack on nuclear forces. Such an attack could be viewed by the targeted state as signalling intent to escalate to nuclear use on the part of the instigator. If the targeted space system enables both nuclear and non-nuclear missions, there is a similar risk of escalation, which has led experts to express concerns about the entanglement of nuclear and non-nuclear weapon systems.[46] Even perceived threats to systems enabling nuclear missions are extremely escalatory.[47] For example, if a satellite were to make a close approach to an NC3 satellite of a rival state without notification or clarification of intent by the approaching state, the rival state may view its NC3 infrastructure as being under threat.

An attack on the ground segment of a system located in the targeted state's territory could also be considered highly escalatory if it entails a breach of territorial integrity. It is less clear how states would respond to attacks on or threats to other types of systems with non-nuclear military uses, which raises questions about further parameters, including about the capability used to attack the system.

Parameter 2. The capability

An attack may use kinetic or non-kinetic counterspace capabilities. Some of these are clearly prohibited by international law or are unprecedented, while others may be used in varying degrees with no consensus on their use under international law. Use of each of these capabilities would therefore incite different responses.

Detonating a nuclear weapon in space would be extremely escalatory because it might signal intent to escalate to terrestrial nuclear use and war. Furthermore, it could be a violation of international law: the 1963 Partial Test Ban Treaty prohibits its parties from conducting nuclear tests, or any other nuclear explosion in space, and the 1967 Outer Space Treaty prohibits its parties from placement of weapons of mass destruction (WMD) in orbit.[48] Arguably, the collective restraint against nuclear tests in space over the past few decades also exhibits crystallization of customary international law against such detonations. In December 2024 the United Nations General Assembly adopted a resolution reiterating the obligation not to place WMD in orbit and further committing not to develop WMD specifically designed

[46] Acton, J. M., 'Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war', *International Security*, vol. 43, no. 1 (summer 2018).

[47] Raju, N. and Wan, W., 'Escalation risks at the space–nuclear nexus', SIPRI Research Policy Paper, Feb. 2024, p. 19.

[48] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Partial Test-Ban Treaty, PTBT), signed 5 Aug. 1963, entered into force 10 Oct. 1963, Article I; and Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty), opened for signature 27 Jan. 1967, entered into force 10 Oct. 1967, Article IV.

to be placed in orbit.[49] The treaty prohibitions, the norm against testing and the 2024 resolution collectively illustrate that the international community would view a nuclear detonation in space as extremely escalatory. Moreover, such a detonation would also have adverse, indiscriminate effects (explored further in parameter 3).

A kinetic strike against another state's satellite could also be extremely escalatory for several reasons. First, a strike on another state's satellite in orbit would be a use of force prohibited by the UN Charter. Second, no state has ever conducted a kinetic strike against another state's satellite. Given the lack of precedent, there is an additional element of uncertainty about how a targeted state may respond. Third, a kinetic strike could also be perceived as escalatory due to the overlap between the technologies for direct-ascent anti-satellite weapons (DA-ASAT) and missile defence systems—DA-ASAT use may be construed by the targeted state as demonstration of missile defence capacity, raising concerns around posturing and preparation for future use of that capability.[50] Several states have confirmed DA-ASAT capabilities, while still more possess missile defence systems with DA-ASAT potential.[51] Moreover, the 'successful' use of such a weapon would create debris in orbit upon striking its target, severely polluting the orbit for not only the attacking state, but also its allies, partners and all other users.

In comparison, non-kinetic methods such as cyberattacks, jamming, spoofing and laser dazzling might appear as less escalatory. However, this depends on further parameters.

Parameter 3. The effects

The effects on the targeted state of an attack (or assumed attack) may be temporary. For example, it may disrupt a space system to undermine its key function at a critical point in a military operation. Alternatively, the attacker may permanently disable or even destroy the system by physically attacking it.

A nuclear detonation in space would be extremely escalatory not just because of the type of capability used (as identified in parameter 2), but also because of its adverse and indiscriminate effects in orbit. Such a detonation would affect satellites in the vicinity and irreversibly disable them. It would also have secondary effects of making that part of the orbit unusable due to debris and radiation. The disastrous effects of nuclear detonations are well-established from tests conducted by the USA and the Soviet Union in the 1950s and 1960s.[52]

A non-kinetic attack can also be escalatory, depending on its effects. For example, a cyberattack on a satellite for non-nuclear communications may have a temporary effect, but it could impair its primary function (e.g. by

[49] UN General Assembly Resolution 79/18, 'Weapons of mass destruction in outer space', 2 Dec. 2024.

[50] Stefanovich, D., 'The indispensable link: Strategic defensive capabilities as a cornerstone of arms control and arms racing', eds T. Zhao and D. Stefanovich, *Missile Defense and the Strategic Relationship among the United States, Russia, and China* (American Academy of Arts & Sciences: Cambridge, MA, 2023) p. 42.

[51] Weeden and Samson (note 26).

[52] Bowen, B. E., *Original Sin: Power, Technology and War in Outer Space* (Oxford University Press: Oxford, 2022), p. 255.

failing to enable uncrewed vehicles at a critical stage). In this scenario, the targeted state may not know how long the attack will last and may not assume that it is temporary. Because such non-kinetic attacks also bolster unpredictability and depend on perceptions and calculations of the targeted state, they can be extremely destabilizing.

In considering effects, even unilateral acts that are not strictly considered 'attacks' can be highly escalatory, such as DA-ASAT missile tests. To date, China, India, Russia and the USA have conducted these tests.[53] Such a test can be escalatory because a rival could perceive it as a demonstration of its adversary's missile defence capabilities and intent to escalate, in addition to the indiscriminate effects of space debris that would endanger the interests of other users of space. Indeed, the adoption in 2022 of a UN General Assembly resolution initiated by the USA suggests that a significant majority of states—155 voted in favour—would view a 'destructive' (debris-creating) DA-ASAT test as extremely escalatory, possibly capable of inciting responses.[54]

Cooperative security ties mean that an attack by one country on a space system of another may have spillover effects in other countries. For example, the USA has raised concerns about cooperation between Russia and North Korea extending to space technology.[55] In the absence of clarity on the intended use of such space technology, this will increase the potential for misperceptions in the Korean Peninsula. Furthermore, such reports can lead states to assume a 'bloc' mentality about rivals, whereby actions of one state may be incorrectly assumed to represent the actions of its allies. In this manner, spillover effects of perceived threats to space systems can exacerbate tensions, possibly even creating new security dilemmas.

The effects of an attack also induce assessment of whether the attack was indeed deliberate or was an accident or false alarm that was misinterpreted. Outer space is a hazardous and challenging environment in which to operate: there is high scope for accidents, particularly collisions; and technical malfunctions and even errors in human judgment are highly probable. The latter includes misinterpretations of data from missile early-warning systems or inaccurate assumptions that a technical malfunction of a system is an intentional attack.

Parameter 4. The consequences

Even if an attack on a space system is not perceived as escalatory based on any of the above three parameters—target, capability or effects—it can have significant consequences for civilians and the environment. These impacts can be escalatory by causing relations between the targeted state and the instigating state to further deteriorate with more gaps in communication. An attack on a space system can have an impact on civilians and the environment in different ways, ranging from merely inconvenient to fatal.

An attack can have immediate consequences for civilians, possibly even resulting in loss of human life or injury. For example, jamming or spoofing

[53] Weeden and Samson (note 26).

[54] UN General Assembly Resolution 77/41, 'Destructive direct-ascent anti-satellite missile testing', 7 Dec. 2022.

[55] Regan, H. et al., 'Blinken warns Russia is close to sharing advanced satellite technology with North Korea', CNN, 6 Jan. 2025.

navigation signals can fatally misdirect an aircraft that is primarily reliant on them for navigation. Attacks can even have long-term consequences (e.g. economic, health and resource-related) that affect a population over time. For instance, space systems can enable national energy sectors and, since electrical power grids increasingly require precise timing data from a GNSS, the interruption of these services could result in widespread power outages.[56] Consequences of an attack can also vary among different segments of a population. In multilateral discussions on space security, the government expert from Canada has underscored how space-delivered data is critical for emergency responses to gender-based violence, asserting that this is one example of disproportionate impacts on differentiated populations, particularly women and girls.[57] Notably, the ICRC has also highlighted legal limitations to attacks on space systems in event of armed conflict under international law, including international humanitarian law.[58] Violation of such legal obligations could therefore also be perceived as highly escalatory.

Attacks also have the potential to harm the environment, both in outer space and on earth, causing a state to endure extensive damage and to incur financial losses. As well as polluting orbits with debris, this also includes debris or uncoordinated rocket re-entries that spread waste on earth. Several such incidents have occurred, notably the re-entry of a nuclear-powered Soviet satellite in 1978 that left radioactive debris over Canada's Northwest Territories.[59] The subsequent recovery and clean-up was a multi-year effort, and Canada ultimately received compensation for the incident from the Soviet Union. The environment is also protected by international law, ranging from general obligations that apply in peacetime to additional obligations that apply during armed conflict. Attacks can thus have environmental consequences that violate international law. In this manner, the nature and the extent of the consequences of an attack on a space system can define whether the targeted state perceives it as more or less escalatory.

Understanding escalation in the context of space systems requires a shared, standardized approach to build common understandings. These four parameters accordingly provide a baseline to enable states to consider how certain attacks or acts may be perceived as more or less escalatory. This framework can be applied and adapted depending on the context. For example, the parameters can be weighed differently depending on the states and regions concerned, their specific administrations and leadership, their known capabilities and the overarching political circumstances. These contextual elements would then provide further insight into the potential response of the targeted state in the scenario, and the likelihood of escalation to follow. In these assessments, the above four parameters are thus a starting point to identify actions deemed more or less escalatory in the space domain.

[56] Doucet and Eves (note 38).

[57] E.g. United Nations, Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, 'Gender-based considerations for a legally binding instrument on the prevention of an arms race in outer space (PAROS)', Working paper submitted by Ashlyn Milligan, GE-PAROS/2023/WP.4, 4 Dec. 2023.

[58] United Nations, General Assembly, Open-ended Working Group on Reducing Space Threats, 'Constraints under international law on military operations in, or in relation to, outer space during armed conflicts', Working paper submitted by the International Committee of the Red Cross (ICRC), A/AC.294/2022/WP.4, 11 May 2022.

[59] Canadian Government, Health Canada, 'Previous nuclear incidents', 3 Sep. 2019.

IV. Recommendations

The above four parameters can inform the design of specific mechanisms for escalation management involving the space domain. The following recommendations suggest a prioritization of measures, focused on reducing the risk of strategically significant systems being targeted, on delineating particularly escalatory actions, and on minimizing the severity of effects and consequences of attacks. In addition, the recommendations acknowledge challenges in implementation of existing laws and norms and propose how they can be improved. The proposed measures are a combination of bilateral and multilateral mechanisms; some of the multilateral-oriented recommendations can be pursued in upcoming United Nations space security processes.

Limit attacks on high-value strategically significant space systems

Mitigating risk entails focusing on the type of space system targeted (parameter 1) as attacks on high-value strategically significant space systems can be extremely escalatory. Accordingly, nuclear-armed states could seek to clarify their intent not to attack NC3 systems. This could be through legally or politically binding commitments, or even by starting with an exchange of views.

An exchange of views could begin with and be steered by the five permanent members of the UN Security Council—China, France, Russia, the United Kingdom and the United States (the P5). Nuclear escalation risks involving space systems fall within the scope of the 2022 P5 joint statement, in which they committed to 'continue seeking bilateral and multilateral diplomatic approaches to avoid military confrontations, strengthen stability and predictability'.[60]

This issue must also be raised in bilateral exchanges among nuclear-armed states. Bilateral arms control agreements have included obligations not to interfere with 'national technical means' of verification, which includes satellites.[61] Bilateral exchanges that recognize the high-value strategic nature of space systems for NC3 therefore clarify the subsequent high risk of retaliatory nuclear use should these systems be perceived as threatened. However, given the current low appetite for formal arms control agreements, the subject could first be broached through Track 1.5 (i.e. mixed official and non-official) and Track 2 (i.e. non-official) dialogues on strategic stability.

Another step towards limiting attacks on strategically significant systems could be to explore reciprocal or conditional commitments to notify in case of unnotified close approaches to space systems. Here, the onus is not only on the approaching state to notify the state whose space system is being approached; a state that perceives its space system as being under threat must also notify the approaching state. Notifications can be shared bilaterally

[60] Joint Statement of the Leaders of the Five Nuclear-Weapon States on Preventing Nuclear War and Avoiding Arms Races, 3 Jan. 2022.

[61] E.g. 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, Article XII; and Russian–US Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START), signed 8 Apr. 2010, entered into force 5 Feb. 2011, Article X.

among states concerned. Additionally, the P5 could commit to establish a multilateral mechanism for such notifications.

This recommendation is not intended to suggest that attacks on other types of space systems are permissible. As parameters 2–4 underscore, there are other considerations that can define whether an attack is perceived as escalatory. However, given that a threat to a space system forming part of NC3 infrastructure could signal intent to escalate to nuclear use, there is value in such bilateral and P5-led discussions, including in the forum of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty, NPT).[62] To increase engagement with states beyond those under the NPT, these commitments could also be made through a UN General Assembly resolution.

Establish common understandings on critical infrastructure

To further reduce risks associated with the type of space system targeted (parameter 1), states should exchange views on how space systems constitute critical infrastructure. This would reduce risk of escalation by introducing more transparency and predictability on how space systems are valued and used in different national contexts.

The term 'critical infrastructure' has not been defined in multilateral discussions on space activities. However, in 2003 the UN General Assembly provided examples of the term in the context of cybersecurity, naming infrastructures used for 'the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health'.[63] Various states have defined critical infrastructure in domestic legislation, which typically includes infrastructure for essential civilian services, national security and defence. Some states, such as Russia, have designated the entire space sector as critical.[64] There is some overlap in the meaning of the term among China, the EU, Russia and the USA, particularly for areas such as information and communications services, energy, transportation and finance.[65] However, the expansive approach of classifying most services as critical may lead to the concept of 'criticality' losing meaning entirely.[66] Nevertheless, continued discussion on critical infrastructure in space security forums would be a useful way to identify areas of commonality.

In December 2024 the UN General Assembly established an open-ended working group (OEWG) on the prevention of an arms race in outer space (PAROS) to advance multilateral discussions on space security in 2024–28.[67]

[62] Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty, NPT), opened for signature 1 July 1968, entered into force 5 Mar. 1970.

[63] UN General Assembly Resolution 58/199, 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures', 23 Dec. 2003.

[64] Russian Federal Law no. 187-ФЗ 'On the security of the critical information infrastructure of the Russian Federation', 26 July 2017 (in Russian).

[65] Su, F., Dovgal, L. S. and Saalman, L., 'Advancing the role of the European Union in promoting global cyber stability', SIPRI Research Policy Paper, Dec. 2023, p. 6.

[66] Su et al. (note 65), p. 6.

[67] UN General Assembly Decision 79/512, 'Open-ended working group on the prevention of an arms race in outer space in all its aspects', 2 Dec. 2024. This OEWG merges and replaces two OEWGs established previously. UN Office for Disarmament Affairs, 'Open-ended Working Group on Prevention of an Arms Race in Outer Space', 2025.

The OEWG will continue work on norms, rules and principles of responsible behaviour from the 2022–23 OEWG on reducing space threats and the 2023–24 group of governmental experts (GGE) on PAROS. The OEWG should discuss measures to protect critical space-based services for civilians (included in the mandate of the previously established OEWG on responsible behaviours). To do so, states can first exchange views on the types of space systems and services that are critical. States must also seek consensus on systems protected by international law for the provision of essential services to civilians.

Characterize acts that are especially escalatory

As noted above, the extent to which an attack on or threat to a space system is perceived as escalatory can also be defined by the type of capability used (parameter 2). Therefore, characterizing the specific capabilities that are perceived as particularly escalatory in multilateral space security forums can help build common understandings on escalation risks. This must be considered along with the effects of an attack (e.g. debris or radiation), how long it will last and the spillover effects if other states are affected. Initial discussion on threats to space systems began in the 2022–23 OEWG and the 2023–24 GGE. However, this discussion must be more systematic if states seek to delineate which types of attack are especially escalatory.

The new OEWG is an opportunity for this discussion. States can exchange views on acts considered especially escalatory (e.g. nuclear detonations in space and kinetic strikes) and acts that may be perceived as escalatory based on their effects (e.g. if a cyberattack on a space system has an impact on end users in other states that are not party to a conflict). Such acts could be considered 'irresponsible behaviour' as discussed in the previous OEWG.[68] These discussions can simultaneously lay the foundation for political commitments to avoid extremely escalatory acts, which can then be considered for inclusion in a future legally binding instrument on PAROS.[69] Notably, avoiding extremely escalatory acts aligns with views raised in the GGE, in particular regarding 'a possible element of a legally binding instrument' to avoid 'Intentional acts/acts that cause harmful interference', especially those 'that pose a particular risk of escalation'.[70]

Enhance resilience of space-based services for civilians

As consequences of an attack may fuel escalation (parameter 4), it is essential to adopt measures that reduce risk of harm. While the first step towards reducing the risk of harm is the above-mentioned exchange of views on critical infrastructure, states must also prioritize resilience of space systems that provide critical services to civilians.

[68] UN General Assembly Resolution 75/36, 'Reducing space threats through norms, rules and principles of responsible behaviours', 7 Dec. 2020, p. 2.

[69] On the history of multilateral discussions on PAROS see Azcárate Ortega, A. and Samson, V., *Counterspace Capabilities: Renewed Hope for Cooperative Governance?*, Centre for International Governance Innovation (CIGI) Policy Papers no. 313 (CIGI: Waterloo, ON, Jan. 2025), pp. 9–13.

[70] United Nations, Group of Governmental Experts on Prevention of an Arms Race in Outer Space, Report, GE-PAROS/2024/CRP.4, 23 Aug. 2024, para. 56(a).

Several actors are already taking such steps. For instance, the EU has multiple priorities for resilience, with examples mentioned in its 2023 strategy including enhancing autonomy in space, identifying essential space systems, identifying major supply chain actors and developing coordinated national preparedness and protocols.[71] Given ongoing efforts towards resilience, states could commit to enhancing resilience of systems that provide critical services for civilians. In conjunction with characterizing certain acts as especially escalatory, this would provide fewer incentives for other states to target such systems and would help minimize the likelihood of such systems being attacked.

The ICRC has proposed practical steps towards this end, for example ensuring that humanitarian workers have uninterrupted multi-system access to satellite services.[72] This is based on the rationale that, if one space system is attacked (e.g. a GNSS such as the USA's GPS), then another (e.g. the EU's Galileo, Russia's GLONASS or China's BeiDou) can ensure continued access. The ICRC has further recommended that states make commitments on behalf of national space agencies and satellite operators to respond to assistance requests from emergency responders and humanitarian organizations.[73]

Build a typology of harms

Minimizing risk of civilian and environmental harms requires a clear understanding of potential consequences (parameter 4). A typology of harms that lays out consequences helps to transform understandings of possible impacts from abstract generalities to concrete cases, thereby driving momentum for protective measures. Such a typology would also reinforce the political backlash and reputational damage that an attacking state may incur if it neglects to consider civilian and environmental harms when conducting military space operations.

Developing a typology of harms could commence with mapping use-cases and space dependencies to understand potential impacts and to distinguish between types of harm. One category could consider direct consequences and immediate impacts—for example, if an attack on a GNSS were to lead to loss of life and injury or if an attack were to disrupt a hospital's emergency services. A second category could consider economic consequences or reverberating impacts that may develop over time—for example, if an attack on a space system were to disrupt financial services and cause severe economic damage to the state, or if an attack were to disrupt a space system on which an agriculture-dependent economy relies. Second-order effects of an attack could then be considered in a different category—for example, if disruption of a GNSS begins snowballing and causes a collision between other satellites that use the GNSS for navigation. Environmental consequences could similarly be categorized into different levels, depending on impact.

Some experts have proposed a consequence-based approach to space governance, recommending that states identify prohibited acts based on

[71] European Commission (note 10), p. 3.

[72] International Committee of the Red Cross (ICRC), 'ICRC observations on the consultants' report *Protecting Essential Civilian Services on Earth from Disruptions by Military Space Operations*', June 2024, p. 3.

[73] International Committee of the Red Cross (note 72).

possible consequences.[74] A typology of harms further extends this rationale and can advance discussions on protecting civilians without prejudice to considerations of including international humanitarian law discussions in space security forums.

Reform state silence and inaction

The parameters presented here point to the need for stronger implementation and enforcement of current international law governing space activities. There are a number of obligations and restrictions on military uses of space that states have failed to uphold and defend. For example, despite the visible rise in non-kinetic attacks on space systems, states have so far employed only political tools in response, primarily issuing unilateral statements condemning the attacks. While states may be hesitant to use stronger legal tools for fear of setting a precedent, state silence and inaction can set a dangerous counteracting precedent—where non-kinetic acts are normalized and viewed as permissible, regardless of consequences.

Several legal mechanisms are readily available under international law—but these remain underused. For example, a cyberattack with widespread consequences (such as the 2022 Viasat attack) and the 2024 jamming incidents are arguably 'harmful interference' under Article IX of the Outer Space Treaty, which empowers states to engage in bilateral or multilateral consultations on such events.[75] Yet, this provision has never been publicly invoked. In addition, states have remedies under general international law in event of 'an internationally wrongful act', particularly countermeasures.[76] Countermeasures allow injured states to engage in conduct that may otherwise be unlawful in order to induce compliance—for instance, freezing assets in its possession to compel the concerned state to act.[77] These tools should be actively used in response to non-kinetic attacks in order to avoid them becoming increasingly acceptable and to build norms against their employment.

Relatedly, despite the inclusive nature of recent space security processes such as the OEWGs—which are open to all UN member states—some states are slow to engage. This may be due to limited resources or to a lack of awareness of space issues and their intrinsic links to strategic stability. However, inaction compromises state interests, particularly of states with newer space programmes and ambitions, as it undermines the treaties and norms that govern space activities. By creating new precedents that are tolerant of harmful interference and weaken international space governance, the rights of other states to equitably benefit from space and to conduct space activities in a stable environment are increasingly threatened. State practice that implements and upholds existing international laws governing space activities is thus essential.

[74] Rajagopalan, R. P., 'A consequence-based approach is needed for space security', The Diplomat, 19 Oct. 2023.

[75] Outer Space Treaty (note 48), Article IX.

[76] International Law Commission, 'Draft articles on responsibility of states for internationally wrongful acts with commentaries: 2001', 2008, p. 126.

[77] International Law Commission (note 76), articles 22, 49–52.

Engage commercial actors and establish accountability

As highlighted above, the private sector can enhance unpredictability in space operations in several ways. To address these, states must exchange views on mechanisms to regulate the companies that enable military space operations. This can help minimize risk of escalation in two ways.

First, it will help states to reflect on how to curtail the arbitrary power that companies have to decide who benefits from services in a conflict. This will also raise considerations on how to establish systems for accountability under international law. Such exchanges will also contribute to overall transparency by encouraging states to provide national perspectives on this specific issue.

Second, there is a need for consensus on when attacks on commercial systems would be legitimate in a conflict. According to experts, commercial space systems can be targets in certain circumstances, comparing them to commercial submarine cables that transmitted national security data in wartime.[78]

Provision of military space services by companies will only continue to grow. These actors differ widely in the types of service they provide as well as in their size, composition, customers, end users and relationships with governments. It is critical to conduct awareness-raising with each of these actors regarding the current laws and norms governing outer space. This is increasingly necessary due to current uses of space in conflicts as company personnel could even be held accountable for war crimes in event of violations of international humanitarian law.[79] The awareness-raising must simultaneously educate the personnel and leading individuals of companies on how their public messaging can be highly escalatory and undermine international (not only national) security and stability.

The upcoming OEWG on PAROS must reinforce applicable laws, including reminding states that the Outer Space Treaty provides that states are responsible for acts of their non-governmental entities.[80] In this regard, the OEWG can initiate an exchange of views on when a state is considered to have effective control over acts of its companies and their personnel under international law. The OEWG could then facilitate exchanges to determine the rights and obligations of companies providing dual-use services in an armed conflict.

V. Conclusions

Military uses of space today exhibit technological advances and a diversity of actors and activities. This is evident from the ongoing war in Ukraine, but also in military operations and conflicts in other states and regions. There are several subsequent avenues that can undermine predictability and transparency in space activities.

The four parameters identified in this paper—the target, the capability used, the effect and the consequences—establish a standardized approach to an initial assessment of whether an attack is escalatory. This assessment can help establish common understandings of escalation risks among states using

[78] Bateman, A., 'The new struggle for space', Englesberg Ideas, 17 Dec. 2024.
[79] Doucet and Eves (note 38).
[80] Outer Space Treaty (note 48), Article VI.

space for civilian and military purposes. The four parameters also inform recommendations to minimize escalation risks. Because the risk of further escalation will be determined by the specific context of any attack, additional variables must be explored, including how the parameters can be adapted to various contexts and how states in those contexts may respond or retaliate.

This would be helped by the development of case studies that illustrate some of the variables determining each context. This includes studies that assess how the parameters would be applied by actors in different states, regions and circumstances. Elaboration of such case studies will be essential, given that pursuit of space capabilities for operational and strategic uses is flourishing across regions. Actors conducting space activities have their own priorities and perceptions, and these differ even among allies and partners. Some of these actors are more willing to push escalation thresholds as regards attacks on strategic assets, and they may continue to do so if they interpret their actions as successful. Given current diverging views on risk and thresholds, escalation management involving space and other domains demands comparison of allied and partner interests in cooperative security arrangements. In particular, this necessitates examining dependencies, perceptions and strategic cultures.

Ultimately, minimizing scope for escalation, including to nuclear use, requires states to address underlying motivations for capability development, whether (and why) they perceive deterrent value in specific capabilities, and understanding how these perspectives inform stances in space security and arms control forums. Meanwhile, standardized assessment of escalation risk in the space domain using the four parameters and their accompanying recommendations can help foster common understandings on risk and can build momentum for escalation management. These recommendations can help slow arms-racing dynamics and reintroduce predictability and transparency in space activities.

SIPRI RESEARCH POLICY PAPER

PARAMETERS TO ASSESS ESCALATION RISKS IN SPACE

NIVEDITA RAJU

CONTENTS

ABOUT THE AUTHORS

Nivedita Raju is a senior researcher in the SIPRI Weapons of Mass Destruction Programme. Her research interests include the space–nuclear nexus, space governance, and transparency and confidence-building. Raju is also a project coordinator on behalf of SIPRI in the EU Non-proliferation and Disarmament Consortium and a contributor to the Alva Myrdal Centre working group on nuclear disarmament in policy and international law.

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

DOI: https://doi.org/10.55163/EDTC6801