SWP Comment
NO. 18 MAY 2026

Resilience as a Response to Russian Threats in Space

Policy Options for Germany and Europe

Juliana Süß

Russian attacks and threat posturing are increasingly extending into space as well. This poses risks to infrastructure in Europe, which is becoming ever more dependent on satellite systems. This affects civilian services such as navigation, but also Europe's defence capabilities. The question is therefore increasingly how such manoeuvres by Russia should be countered, and whether weapons systems should be deployed in space as a deterrent. Europe's armed forces are far more dependent on space systems than the Russian armed forces. Given this asymmetry, Germany and its partners should focus primarily on the resilience of their satellite systems.

Attacks on satellite systems are neither rare nor merely an abstract threat, but a common tactic used to undermine the European security architecture. At the end of 2025, the British Ministry of Defence reported weekly attempts by Russia to jam military communications satellites. In February 2026, it emerged that Russia was also believed to have conducted signals intelligence operations against communications satellites used by the Bundeswehr.

Deterrence as part of German defence policy

In a satellite system, the satellite in space, the ground station on Earth, and the signals transmitted between them are all potential targets that must be protected against sabotage, attack, interception, and other forms of interference. Otherwise, critical military capabilities such as communication, navigation, reconnaissance, and missile early warning systems risk being temporarily or permanently disrupted, with far-reaching consequences. For example, target identification and command and control could be impaired, delayed, or lose precision. Civilian functions could also be impacted, including emergency call systems, data transfer in the banking sector, and the provision of meteorological data. For this reason, satellite systems are of strategic importance for a modern state. The protection of these systems requires a sound conceptual foundation.

The Federal Government regards deterrence as an "integral component of a comprehensive security architecture". In its

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

National Security Strategy of 2023, the German government cited attacks on space systems as an example of why deterrence must be comprehensive and operate across all domains. The German Space Safety and Security Strategy, published in 2025, identifies deterrence (together with defence preparedness and resilience) as one of the three fields of action. According to the document, Germany shapes its deterrence posture in space through a combination of international diplomacy and partnerships, resilience measures, defence readiness, and military capabilities.

The German government thereby reserves the option of employing military means to deter Russia in particular from carrying out attacks in space. However, the details of potential measures that could be used are not mentioned. The use of kinetic weapons is to be ruled out, as the Federal Republic has already signed a moratorium on the testing of kinetic anti-satellite (ASAT) weapons and therefore will not test military capabilities that generate space debris. Yet even without such "hard-kill" methods, a range of alternative ASAT weapons and measures remains available that could be used to impair hostile satellites in the course of potential counter-attacks. This suggests that the Federal Government is now evaluating some of these non-kinetic options.

By procuring capabilities at the less escalatory, non-kinetic end of the ASAT spectrum, Germany would have a "sword" at its disposal with which to hold its own against adversaries in space. The acquisition of military space capabilities could signal to Russia that an attempted attack on German infrastructure might potentially trigger a counter-attack against Russian satellites. However, it would be mistaken to assume that such a threat would actually have a deterrent effect on Moscow. The main reason is that the loss of Russian satellites would do little to constrain the country's military capabilities.

Adapting to the adversary

Russia is considered the "most immediate threat" to Germany. Accordingly, a deterrence policy is required that is adapted to this threat and takes into account the means at Russia's disposal and how it would be likely to operate in a potential conflict. In the domain of space, there is an asymmetry between Russian and Western capabilities. Although Russia possesses satellite systems, it has integrated them into its military infrastructure only to a relatively limited extent. This also constrains a potential Western deterrence strategy.

Russia is far less dependent on space systems than Germany and its partners, which at the same time significantly limits Moscow's military capabilities. For instance, Russian forces experience difficulties in communicating effectively. In addition, they face challenges related to battle damage assessments, which in turn affects military planning. Given that Russia's space industry is struggling economically, this situation is likely to become even more pronounced in the coming years. By contrast, Western dependence on satellite systems will continue to grow, as the concept of "Multi-Domain Operations" (the orchestration of military activities across all domains) is already being implemented within NATO.

There are indications that Russia is attempting to close its capability gaps. According to reports, Moscow has been seeking to acquire satellite imagery on the commercial market since April 2022. Moreover, Ukrainian intelligence services have accused China of using its technologically superior satellite systems to provide Russian armed forces with targeting information in the war in Ukraine. Beijing and Moscow deny these allegations. A Chinese satellite-imaging company has also been sanctioned by the United States for allegedly passing radar imagery to the Russian mercenary Wagner Group. If these cases are confirmed, this would imply that Europe, should it employ offensive measures, might also have to contend with Chinese satellite systems.

However, even a temporary and non-kinetic interference with the satellite systems of a third country would entail risks and constitute horizontal escalation. The consequences of such an escalation would be difficult to calculate, particularly in view of the advanced kinetic ASAT weapons possessed by China (as well as Russia). Therefore, a different approach is required.

Resilience as a deterrence measure

Russia's calculations in space can be influenced in other ways. To deter Moscow from launching an attack, measures can be taken that hamper access to potential targets, thereby reducing the likelihood of a successful attack. Europe should therefore rely on resilience rather than on offensive measures.

The key lies in establishing a system that prevents the complete disruption of critical services. Protecting satellites is complex and can entail high costs. For example, it would be very difficult to protect a satellite against a direct kinetic attack by an ASAT missile or even against the detonation of a nuclear weapon in space. Therefore, the focus should be placed on resilience, both for individual satellites and for constellations, meaning entire groups of satellites. The German Space Safety and Security Strategy already addresses this, even if it does not go into detail.

The resilience of individual satellites can be enhanced in various ways. One option is to frequently change transmission frequencies ("frequency hopping") or to strengthen the resilience of cyber systems. Another approach is to improve space situational awareness, enabling the early detection of potential interception attempts and physical interference. Satellites can also be hardened against elevated radiation levels and electromagnetic pulses, which provides a degree of protection against the effects of a nuclear detonation. Hardening against electromagnetic pulses increases production costs by up to 10 per cent, while hardening against radiation raises them by approximately 2 to 5 per cent. Satellite constellations can also be made more resilient, for example by enabling inter-satellite communications, such as via laser links, in order to bypass ground stations. Satellites can also be deployed in multiple orbits in order to reduce the risk of damage from potential collisions.

The objective is not to equip every individual satellite with all conceivable protective measures. Rather, the aim is to ensure the continuity of service so that individual failures can be compensated for. This is achieved by creating a "system of systems" composed of multiple layers. These include products from commercial providers, which can provide services rapidly but are not protected against all types of attacks (not least for economic reasons), as well as military satellites (including those of partners), which are more heavily protected. Manual or terrestrial alternatives also form part of this architecture. This requires the appropriate hardware, for example terrestrial long-range navigation systems. In addition, the systems must be interoperable, with common interfaces and standards. Beyond that, it is necessary to determine which satellite services must be available at all times and under all circumstances. These services must then be protected and hardened accordingly.

The commercial Starlink constellation is a good example of how resilience can be implemented in practice. The communications network has proved highly useful to Ukrainian forces in the war with Russia, despite several attempts by Moscow to disrupt the service through electromagnetic interference and cyberattacks. SpaceX, the company behind Starlink, primarily relies on software updates to respond to such attacks. This case demonstrates that rapid adaptation in this domain can be sufficient to counter hostile actions. Although the exact costs of these modifications have not been disclosed, software updates are primarily associated with personnel costs.

In addition to advanced jamming systems and cyber capabilities, Russia also possesses kinetic space weapons. However, an attack on a large satellite constellation using such weapons would require signifi-

cant resources and entail serious risks for partner states. Even smaller constellations confront Moscow with a similar dilemma. Russia is therefore more likely to carry out attacks primarily targeting the electromagnetic spectrum and cyberspace. This approach requires relatively few resources and has proven successful elsewhere. The costs of resilience must be weighed against the potential costs of escalation and the difficult-to-calculate consequences of an offensive response to Russian manoeuvres. In that comparison, the former option has a clear advantage.

Resilience as a European strategy

The German government's new investments in the development of space capabilities, along with corresponding Europe-wide initiatives, come at the right time to create resilient structures. Resilience also serves to deter Russia, as it can help shield targets from attack or make attacks more costly for the aggressor, both politically and materially. Protective measures are already being incorporated into the planning of major satellite architectures; this applies to the European Union's proliferated IRIS2 constellation and to the Bundeswehr's planned SatComBw4 communications constellation. The Bundeswehr also intends to network the latter using laser communications to enable interoperability. The European Launcher Challenge, in turn, is intended to drive forward the European launch market and, in so doing, also improve the ability to replace satellites quickly. Furthermore, the Bundeswehr and NATO have begun to integrate commercial providers into their military reconnaissance infrastructures. This approach should be maintained and expanded.

However, there are other ways to protect satellite services. Within the Alliance, the exchange of space situational awareness data should be improved so that partners can warn one another of threats more quickly. NATO exercises that incorporate service disruptions into their scenarios also help to build resilience. The German government should support commercial companies with information, including on attempted attacks against state systems, so that protective measures can be tailored more precisely. This applies equally to companies that do not serve a direct defence purpose. Consideration should also be given to ordering replacement satellites at the time of procurement, so that they are available in the event of failure. The initial malfunctions in the SARah reconnaissance constellation show that failures are not caused exclusively by attacks and that other forms of disruption must also be anticipated. Terrestrial options, such as long-range navigation systems, should be considered wherever possible. They provide additional security and available alternatives in the event that satellite services are disrupted.

Juliana Süß is an Associate in SWP's International Security Research Division. This Comment was produced within the framework of the Strategic Threat Analysis and Nuclear (Dis-)Order (STAND) project.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2026C18

(English version of SWP-Aktuell 21/2026)