REPRESENTATIVE of German Industry + Trade

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

**International Competition and Norms in Space and Cyberspace:**
**Perspectives for German Industry**

Outer space and cyberspace are both becoming increasingly essential domains for commercial activity. At the same time, they have also become domains of strategic and geopolitical competition among states and other actors. To access the benefits from space and digital services, business must navigate an international environment fraught with tension and abide by often ill-defined or contradictory sets of rules. The purpose of this paper is to provide an overview of relevant norms in space and cyberspace as well as a look at their relationship to international political dynamics. Trends on the international stage have a profound effect on German industry, including in these emerging sectors. Throughout the paper, I will include positions and perspectives from German industry on relevant space and cybersecurity issues. My aim is to provide insights to a transatlantic business and policy audience on how German companies and industry associations are navigating current international trends in space and cyberspace, with the hope of fostering collaboration on shared challenges.

## Space

### Background

As of this writing, there are over 6600 satellites in Earth orbit, about 4000 of which are active. Space systems generally provide services related to earth observation, navigation and positioning, or communication. Information from space systems is used for commercial purposes ranging from transportation, efficient agriculture, broadcast and internet communications, real-time financial transactions, to climate science and weather prediction. The driving trend of the last decade has been the phenomenon of 'New Space' – the increasingly commercialization of space activity and entrance of new market players apart from traditional aviation and defense contractors. The expansion of the space sector has led to an increase in the pace of satellite launches and increased the pressure for international standards and regulation in Earth orbit.

Space technologies have always been strategically relevant. Rockets can place civilian satellites in orbit or deliver nuclear warheads. Earth observation satellites can provide accurate maps of cities or military installations. GPS can guide pizza delivery to your house or a cruise missile. Given the dual-use nature of space technologies, countries often impose export controls and domestic content requirements for state-funded projects to reduce dependence on foreign providers. Despite the proliferation and 'democratization' of access to space, launch capabilities remain prohibitively expensive for much of the world, with only a small collection of countries and firms maintaining the ability to place objects in space.

### International Space Norms

International governance in space comes from patchwork of treaties, non-binding agreements, and bilateral or multilateral initiatives. Below is a list of the most relevant treaties and guidelines from an industry perspective. While there is a lively international debate on space mining and resource extraction in space, this sector remains for now largely theoretical. As such, I focus on the governance of

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

Earth orbit. The agreements below come from the UN Committee on the Peaceful Uses of Outer Space (COPUOS) and are administered by its secretariat, the Office of Outer Space Affairs (OOSA).

- *Outer Space Treaty,* 1967: The foundational treaty on space conduct. It establishes the principles of free access to space and the use of space for peaceful purposes. It prohibits the placement of weapons of mass destruction in space and claims of sovereignty on the Moon or other celestial bodies.
- *Liability Convention,* 1972: establishes the liability of 'launching states' for damages caused by objects placed into space and sets the procedures for settlement of claims for damages.
- *Registration Convention,* 1975: establishes the responsibility of launching states to register space objects and provide information to their orbits and general purposes.
- *Space Debris Mitigation Guidelines,* 2008: A voluntary set of guidelines meant to reduce the generation of space debris. It includes a requirement to safely dispose of spacecraft after the end of their missions and prohibits the intentional destruction of satellites.

Currently, there is little impetus towards a new treaty on space activities. Disputes over standards and cost-sharing between the established space powers and the global south prevent a binding agreement on debris mitigation measures. The European Union has proposed a voluntary Code of Conduct for Outer Space Activities, which many nations agreed with in principle, but thus far it has failed to gain international support. Russia and China have proposed the Treaty on the Prevention of the Placement of Weapons in Outer Space (PPWT). The US is intensely skeptical of the PPWT, as its definition of space weapons would ban defensive systems on satellites but not antisatellite weapons. The US has also declined to endorse the EU's Code of Conduct and has proposed its own norm framework through the Artemis Accords.

- *International Code of Conduct for Outer Space Activities (EU)*: a set of non-binding guidelines for space activities initially proposed by the EU in 2008 with several iterations since aimed a promoting the peaceful and responsible use of space. Key aspects of the Code of Conduct include commitments transparency and reduction of orbital debris creation.
- *Artemis Accords (USA)*: a set of voluntary principles set forward by the US and implemented through bilateral agreements with partner countries. Signatories to the Artemis Accords commit themselves to transparency, the peaceful use of space, orbital debris mitigation, and interoperability in their space systems among other principles. There are currently 12 signatories to the Artemis Accords, including the UK, Italy, Luxembourg, Japan, and South Korea.

Orbital Debris

As noted in the background, the number of objects in Earth orbit and the rate at which they are being added have both dramatically increased over the last decade. With the expansion of the space sector and plans of companies like StarLink, OneWeb, and Amazon's Project Kuiper to provide internet services from megaconstellations of potentially tens of thousands of satellites in low Earth orbit, the issue of orbital debris has taken on new relevance. Orbital debris includes space junk like inoperative

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

satellites which have reached the end of their service life or detritus from launches such as spent boosters or explosive bolts. These objects can remain in orbit for years maintaining their orbital velocities of >25000 km/h, which means collisions from even miniscule items can cause significant damage to a satellite or spacecraft. NASA's Orbital Debris Program Office estimates there 500000 ~1 cm objects in Earth orbit and over 100000000 1 mm or smaller.

Debris mitigation is therefore crucial to the continued use of space. Governments, companies, and organizations around the world have taken steps to mitigate their creation of new debris and are developing technologies to remove existing debris. Space agencies and private networks are also expanding their space situational awareness (SSA) capabilities to track objects in Earth orbit using ground and space-based sensors. As a comprehensive picture of the orbital environment requires sensors around the globe, SSA is an area in which international cooperation is essential.

Two of the largest single increases in orbital debris came from a 2007 test of a Chinese antisatellite missile and the 2009 collision of an active communication satellite with a derelict Russian military satellite. Both incidents generated thousands of pieces of debris which will remain in orbit for decades, which highlights the vulnerability of the orbital environment to conflict or accident.

Dual-use Technologies and Export Controls

Space technologies, especially launch systems, are inherently dual use, meaning they can have either military or civilian/commercial applications. As such, countries often impose export controls on space-related technologies. Given the US' position as the predominant space power (over half of the active satellites in orbit are American), US policy carries outsized weight in the space sector. Below is a quick overview of US and international export control regulations as they pertain to space.

- *International Trade in Arms Regulations* (ITAR): Managed by the Department of State, the ITAR governs the import and export of defense articles by the United States. In addition to covering conventional weapons such as firearms, the ITAR also covers rockets and space launch vehicles in Category IV. Any person who seeks to export or import rockets or their components, including engine parts and guidance systems must attain approval from the State Department's Directorate of Defense Trade Controls.

- *Wassenaar Arrangement*: an arms control body with 42 member countries, the Wassenaar Arrangement maintains a Munitions List and a List of Dual-Use Goods and Technologies, which includes Aerospace and Propulsion. Wassenaar member countries enact export controls on covered items and technologies through national regulations.

Space and German Business

In 2020, the Federation of German Industries (BDI) proposed a *Weltraumbahnhof* (literally "space train station," hereafter translated as spaceport) from a ship-based launch platform in the North Sea. The aim would be to take advantage of the trend towards miniaturization in the space industry to allow Germany to fill a niche for small payload launches under one metric ton. With a North Sea spaceport, Germany and Europe would gain a layer of resilience and autonomy in their strategic space capabilities

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

and reduce costs for European commercial space service providers seeking access to low Earth orbit. "Responsive Space" is an emerging field within the space industry wherein satellites are assembled and launched on relatively short timelines to meet immediate needs. In the case of conflict or emergency, a responsive space capability would allow Germany and Europe to replace or increase communications or Earth observation capabilities with little lag time. A small sea-based launcher like the kind BDI proposed would be well suited to responsive space missions.

Space services present a wide range of commercial opportunities for German companies in every sector. Earth observation and position data help improve efficiency transport and logistics and promote sustainable agriculture practices through smart farming. Satellite-provided internet also helps to drive the emerging internet of things and networked manufacturing (Industry 4.0). Demand for commercial space services will of course continue to drive expansion in the space sector itself with the need for more satellites and rockets to launch them.

**Cyberspace**

Background

The world's growing dependence on digital products and services is a trend so large it hardly needs mention. Along with the expanded capabilities the proliferation of networking and computer technology has brought have also come a host of vulnerabilities. Those vulnerabilities were put on stark display across the first half of 2021 with a string of high-profile ransomware attacks on businesses in the US and Europe. The number and cost of cyberattacks is also increasing. The German technology industry association Bitkom estimates that cyberattacks have cost the German economy 223 billion Euro in 2021 alone, a 358% increase from 2019. With the increasing economic damage from cyberattacks comes pressure for policymakers and industry to mitigate vulnerabilities to illicit cyber activity.

Many cybercriminals work with implicit state sanction. State intelligence agencies across the world also engage directly in cyberespionage, sometimes for the purpose of stealing intellectual property or trade secrets. The secret and illicit nature of cyber threats makes them difficult to address directly, but countries and businesses are working to harden their systems against ransomware and other incursions. Internationally, authorities are taking steps to crack down on cybercriminals' funding sources and reduce their safe havens where possible.

Geopolitical Competition and Cyber Norms

A 2020 report from the Carnegie Endowment for International Peace identified four principal hinderances to the development of international cyber norms: 1. Low barriers to entry in cyber-activity 2. Lack of transparency in state activity 3. A dearth of great power cooperation 4. A lack of clear incentives for internalizing norms. In the current international environment, there is little trust between the main cyber powers, as well as a plethora of non-state groups with varying degrees of affiliation to state patrons. The inability to definitively assign responsibility in many cases makes the development and enforcement of norms in cybersecurity difficult. Meanwhile, the problem is becoming increasingly acute with the number and severity of cyberattacks increasing year over year.

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

Such norms as do exist govern state activity both in terms of actions directly taken by states as well as the export of cyber-relevant technologies such as software or surveillance devices. In 2013, the Wassenaar Arrangement expanded to include cybersecurity items, such as intrusion software, which are now subject to export controls like other dual-use technologies. The NATO Cooperative Cyber Defence Center of Excellence maintains the so-called Tallinn Manual, a definitive overview of the application of international law to cyber operations in conflict and during peacetime.

The UN organized a Group of Governmental Experts (GGE) on cybersecurity in 2013, 2015, and again for proceedings across 2019-2021. While GGE recommendations are widely respected, there is little evidence of norm adoption from changes in state behavior based on the GGE recommendations. The UN also organized the so-called Open-Ended Working Group (OEWG), which included a wider variety of stakeholders from industry and civil society. The OEWG originated as a Russian proposal as an alternative to US calls for another GGE. In its final report, the OEWG called for confidence building measures between states to improve trust on cyber issues and proposed a framework for regular institutional dialogue in the future.

There are also industry-led norm creation efforts, such as Microsoft's Cybersecurity Tech Accord or the Siemens-led Charter of Trust. Both initiatives lay out sets of principles for their signatories centered on promoting overall security and protecting users. They also establish frameworks for cooperation between businesses and present common positions in multi-stakeholder fora.

US Cyber Policy

In May 2021 the Biden Administration issued an Executive Order on improving US cybersecurity. The EO directed reviews from several federal agencies on their cybersecurity strategies, a modernization of federal cybersecurity practices, and closer cooperation with the private sector both on incident reporting and the implementation of security standards. Since May, the Administration has also announced efforts together with the private sector to train and expand the US cybersecurity workforce.

The Biden Administration calls addressing cyber threats a 'whole-of-nation effort' in addition to its 'whole-of-government' approach. Along with actions to improve cybersecurity directly, the Administration is also attempting to step up enforcement actions against cyber criminals, including cutting their funding sources. The Treasury Department has issued new sanctions guidance on virtual currencies and in September targeted a virtual currency exchange for its role in facilitating payments to ransomware actors.

EU Cyber Policy

In March 2019, the Commission published a Toolbox for 5G Security, which laid out guidelines and standards for member states to assess risk in their next generation networks, and was fully implemented in the summer of 2021. The European Commission and the High Representative for Foreign and Security Policy released a new Cybersecurity Strategy in December 2020. Like the US, the EU strategy also calls for an expansion of European cybersecurity capabilities and increasing resilience in critical infrastructure. The EU has also employed its sanctions power in combatting cyber criminals, placing sanctions on individuals related to attacks on the Union or its member states.

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

The EU has also put forward a Programme of Action for Advancing Responsible State Behaviour in Cyberspace (PoA) at the UN similar to its proposed Code of Conduct for Space Activities.

Cybersecurity and German Business

Germany's highly developed export-oriented economy is especially vulnerable to cyber threats. German companies' competitive advantage often comes from their intellectual property and human capital, making the theft of patents or employee data even more damaging. Cyberattacks can also lead to broader supply chain disruptions as demonstrated by Colonial Pipeline attack in the summer of 2021. The Federation of German Industry has therefore called for stronger cyber protections of the entire German economy by the German government, as well as on the European and international levels.

Companies of all sizes are targets of malicious cyber activity. Going forward, even small and midsized enterprises will need to devote more resources to cyber defense and resilience. Addressing the ever-increasing economic costs from cyberattacks will take coordinated action from industry and governments, especially in promoting effective standards and in training a large and capable cybersecurity workforce.

**Priorities for German Business**

What do the trends in space and cyberspace mean for German companies going forward? Below is a quick overview of commercial and policy opportunities German businesses face as these fields mature.

*Space*

- Rocket and satellite manufacturing: with the potential for a North Sea spaceport, Germany is well positioned to fill a market niche in the manufacture and launch of small satellites into low Earth orbit.
- Increased use of space services: as the commercial space sector grows, so will access to services from space systems. Real-time earth observation and satellite-provided internet promise significant benefits to large and small companies alike.
- Space sustainability: German firms and policymakers can continue to be at the forefront of developing and implementing debris mitigation measures in Earth orbit and developing orbital debris removal technologies.

*Cyberspace*

- Workforce development: the German apprenticeship system is an attractive model in many countries. To ensure a large and skilled cybersecurity workforce, German firms and industry associations can lead by example in reskilling and upskilling workers in this expanding field.
- Standard setting: industry best practices can lead the way for later norms and agreements. Initiatives like the Charter of Trust provide a responsible industry voice on international cybersecurity standards.

REPRESENTATIVE of German Industry + Trade

1130 Connecticut Ave, Suite 1200
Washington DC 20036 | USA
(001) 202 659 4777

**Conclusion**

Space and the internet have still only realized a fraction of their potential commercial benefits. Information and space services enrich all our lives every day, but they have also exposed businesses, individuals, and nations to a variety of new vulnerabilities and risks. The competitive international environment exacerbates the danger of politically driven disruptions in space or information infrastructures from conflict or malicious activity. It is incumbent on industry and policymakers to understand and mitigate these risks. International laws and norms are one way to do that, but they are only as effective as their stakeholders, public and private, make them.

**Your Contact**

Jay Morgan
Policy Manager

Representative of German Industry and Trade (RGIT)
1130 Connecticut Ave NW, Suite 1200 | Washington, DC 20036
Phone (cell): +1 202-378-6900 | Phone (direct): +1 202-659-6822
E-mail: jmorgan@rgit-usa.com | Web: www.rgit-usa.com/en/