Space Competition 2022

Ralph D. Thiele

April 2022

Summary

Competition in space is heating up as critical services on Earth increasingly depend on the collection and transmission of data by satellites. New technologies and capabilities have become a particularly dynamic driver of relevant developments. Not only non-governmental actors are grasping upcoming opportunities. Consequently, the panoply of threats to space systems keeps evolving dynamically. In particular countries such as Russia and China have developed and tested a wide range of counter-space technologies that could restrict Western access and freedom to operate in space. NATO and the EU to define collective positions, approaches, systems, and tools to protect their interests in space, both as a continuing factor in growth, prosperity and innovation, but also to secure it in a complex, dynamic and worsening security environment.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

1. Heading

The space sector is in the midst of a massive transformation. Increasingly, critical services on Earth depend on the collection and transmission of data by satellites. Space-based capabilities deliver a wide range of effects that underpin daily life. It is also of key importance for upcoming multi-domain military operations.

Clearly, geopolitical rivalries between major powers such as the United States of America (USA), China and Russia have an impact on space. As competition is growing, strategic competitors seek to undermine NATO's and the European Union's (EU) political and military-strategic objectives by deploying increasingly sophisticated strategies, often through well-orchestrated political, military, economic, social, infrastructural and information efforts. New technologies and capabilities have become a particularly dynamic driver of relevant developments creating increasingly feasible operational realities of warfare to include the space domain. In the commercial sector, mega-constellations are developing with disruptive technologies as catalysts.

2. Threats

Serious threats to space infrastructure are relatively new phenomena. For a long time, space assets were protected by an invisible fence. As more countries and commercial firms have begun participating in satellite construction, space launch, space exploration etc., new risks and threats have emerged. Consequently, space has evolved into a contested and congested operational domain, where opponents would attempt to attack Western capabilities, by jamming or hacking information and communication systems.

Chinese and Russian military doctrines underline the importance of space for modern warfare. Both states want to use their own capabilities to limit the military effectiveness of the US and its European allies and have implemented this goal by means of military reorganisation. To China and Russia, space superiority is considered to be part of the ability to control the information sphere as a key component of modern warfare. Winning the battle in orbit will be decisive in future warfare. A particularly interesting perspective is that they consider space, cyberspace, and electronic warfare as integrated capabilities.

Both countries have developed robust and efficient capabilities, including space-based Intelligence, Surveillance, Reconnaissance (ISR), as well as improvements to space launchers and satellite navigation constellations. These provide for monitoring enemy forces and deploying own forces in a targeted manner. The Chinese and Russian space surveillance networks are ideally suited to search for, track, and classify third countries satellites. Both states have an impressive portfolio of cyber and electronic warfare (EW) capabilities, energy weapons and ground-based anti-satellite (ASAT) missiles. Robust and capable space services provide their militaries with the ability to command and control their forces worldwide. Enhanced Situational Awareness enables them to monitor, track and target opposing forces. Own global positioning system satellite networks support own operations.

In a number of critical space technologies, such as quantum, cyber and electronic warfare, China and Russia already have an edge over the West. This tends to increase due to the proliferating effect such technologies have upon each other. China's success in satellite-based Quantum Key Distribution (QKD) – delivering next-generation encryption keys to networks in geographically dispersed areas – is a shining example of what should be expected.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

When looking at China´s general approach to space, its journey towards a strong space presence goes far beyond military capabilities. It includes a space transport system, space infrastructure i.e., satellite remote-sensing systems, satellite communications and broadcasting systems, and satellite navigation systems. Manned spaceflight has an important role, as well as deep space exploration such as lunar exploration, planetary exploration, space launch sites and telemetry, tracking and command. China's space station in Earth orbit - is scheduled to be completed by the end of 2022.

Against this background, ensuring the confidentiality, integrity and availability of Western space assets and space data has become a critical new challenge. Yet, the digital dependence of NATO and EU along with its rather "pedestrian" digital performance constitute a significant weakness. The new space environment features adversaries that seek to disrupt space systems in order to severely degrade the capabilities of the armed forces to achieve their mission in the context of growing reliance on space capabilities, in particular data gathering, navigation and synchronization. Vis-à-vis their highly sophisticated technological competence, sovereign space systems have become an "Achilles' heel" for NATO´s and the EU´s armed forces.

Another weakness is the high dependence on civilian space systems for key services, especially telecommunications. For example, 90% of US military telecommunications are routed through civilian assets, which lack the shielding, protection, and overall resilience of military satellites.[1] This is a result of the powerful expansion of military consumption of space services and is just one instance of military reliance on civilian critical infrastructures.

Among others, cyber threats have come to the fore. In addition, recent trends such as software-defined satellites, usage of COTS components, in-orbit reconfigurations, intelligence on board, quantum technologies, etc. are making space assets and data more and more vulnerable to cyber-attacks.

3. New Business

The massive increase in satellite capacity will continue to change the ways in which satellite operators can sell capacity to end users. Whether it is cloud networks, flexible capacity, dynamic beam-switching ground terminals, or other aspects, satellite operators and the ensuing value chain are rapidly developing new technologies that will allow satellites to become ever more attractive to a wider market.

GEO satcom operators have developed wholly new satellite designs, fleet architectures, and ways of engaging with customers that enable greater system-level flexibility and responsiveness. Established satcom operators, such as SES with o3B and its MEO fleet, and Telesat with their planned LEO constellation, have developed digital-enabled satellites for medium and low earth orbit (MEO and LEO). Further impressive projects have been developed by newcomers, such as One Web, Starlink (SpaceX) and Kuiper (Amazon). These developments highlight the ongoing transformation in space and constitute a significant upgrade from geostationary earth orbit (GEO) satellites.

Clearly, small and nanosatellites will populate LEO in the coming years. They have evolved from 'toys' produced in small university laboratories to highly sophisticated, software-defined supercomputers in space, capable of fielding giant networks of sensors, listening in to the radio-frequency emissions of Earth or capturing 'signals of

[1] Easton, I. (2010), The Great Game in Space - China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy. Project 2049 Institute, http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

opportunity' generated by other satellites in space. The sector is characterised by rapid evolution and constant improvement.

With the expansion of the Internet of Things (IoT) – in sectors as diverse as defence and security, transport, oil and gas, and agriculture – business-critical information from tens of millions of objects will need to be sent to and from areas that are not served by terrestrial networks. LEO is particularly well-suited to narrowband connectivity, processing signals emitted by connected objects. It offers a satellite link anywhere in the world, complementing low-power, wide-area, wireless technology (LPWA) IoT terrestrial networks, without increasing the cost or energy consumption of the objects. MEO is becoming popular, as the O3b constellation has proven that they can deliver immense bandwidth, telecommunications, and Internet connectivity services at a fibre-like speed across the globe for regional networks, but also on-the-spot and difficult to jam connections for diverse mobile users, such as special forces and passengers on cruise ships. This orbit includes a low latency needed for real-time applications in 5G networks and reduced propagation loss.

The close proximity of LEOs and MEOs to Earth allows them to deliver ultra-high bandwidth to customers. MEOs and LEOs support real-time command & control. They transport data from UAVs and ISR systems to analysis centres in headquarters anywhere in the world. The use of AI and Big Data will simplify the use of satellite imagery solutions to track and counter terrestrial threats.

Laser communication will be a game-changer for the satellite imagery industry. The integration of satellite IoT and the Galileo navigation system will improve the performance of drones used mainly for surveillance and tracking the movements of various military assets. Secure embassy communications, police, intelligence, and special forces requirements are perfect fits. Satellite technology is also evolving to play a larger role in Public Protection and Disaster Relief (PPDR) and Common Security and Defence Policy (CSDP) missions.

4. Space Architecture

With view to emerging capabilities and interoperability requirements it can be expected that the evolving US space architecture will shape the respective endeavours of NATO, the EU, and their member nations. While the USA will still develop and employ large satellites such as GPS and protected communications for strategic missions, it plans to proceed with building a new military space architecture designed to support operational tasks with a focus on small satellites.[2]

The envisaged US architecture is composed of seven "layers." These layers are supposed to feature up to 400 small spacecraft that can be quickly replaced if needed. This will significantly strengthen their resilience, as opponents will be prevented by the sheer numbers from destroying entire systems. Resilience will further be increased, with the involvement of multiple satellite makers. Each layer will support given operational tasks.

The "support layer" is supposed to enable a common, resilient ground support infrastructure in order to facilitate the space-based capabilities of the other layers to transmit, receive, process, exploit and disseminate data.

The **"transport layer"** is a space-based **communication** system for all the other layers that is supposed to provide assured, resilient, low-latency military data and connectivity worldwide to the full range of military platforms.

[2] https://www.nationaldefensemagazine.org/articles/2019/9/19/details-of-the-pentagon-new-space-architecture-revealed

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The "**tracking layer**" will deal with advanced missile threats and will provide global indications, warning, tracking, and targeting of advanced missile threats, including hypersonic missile systems.

The "**custody layer**" will accelerate the sensor-to-shooter interaction and sense and track objects on the ground down to the size of trucks and provide target-related information directly to weapon systems.

The "**deterrence/emerging technologies layer**" is an enhanced space situational awareness (SSA) capability that also covers space from geostationary orbit to the region around the moon where traffic is increasing, but not well monitored yet. It is supposed to incubate new mission concepts to deter hostile action in the increasingly active region extending beyond the geosynchronous belt to lunar ranges.

The "**battle management layer**" will provide autonomy, tipping and queuing, and data fusion for mission command & control to include time sensitive targeting.

The "**navigation layer**" will provide alternate positioning, navigation, and timing (PNT) for Global Positioning System (GPS)-denied environments. It is intended to come up - similar to the battle management layer - with onboard processing to provide navigation and launch data to the other satellites.

5. Opportunities

The use of satellite applications for commercial and defence sectors presents numerous opportunities. After NATO in 2019 declared space to be a new operational domain, alongside land, sea, air and cyber, they released an Action Plan, which aims prepare the Alliance to be capable of operating in a "contested, congested and competitive space environment."[3] To implement space as an operational domain, NATO is enhancing its space domain awareness and common understanding of the space environment, including threats and risks. Maintaining situational awareness and reliable access to space services are critical to ensure the success of NATO's operations, missions, and activities. The Alliance has started integrating space in training and exercises, operational planning, capability development, as well as in its innovation initiatives.

As emerging technologies keep transforming the space domain, NATO will take advantage of these developments to maintain its technological edge. NATO´s New Space Policy has integrated space into NATO's core tasks, serving as a forum for political-military consultations and information sharing on threats, challenges, vulnerabilities, and opportunities, as well as the development of legal and behavioural norms. Thus, an effective provision of space support and effects to the Alliance's operations, missions and other activities will be ensured. The development of compatibility and interoperability between Allies' space services, products and capabilities will be facilitated.

In early 2021, NATO leadership adopted the NATO Warfighting Capstone Concept (NWCC). It addresses temporal, spatial, functional, and structural aspects of the Alliance's approach to warfare development and warfighting with a 20-year horizon. The NATO of tomorrow is preparing for a multi-domain, -regional and -instrumental context. It understands it has to adjust to the convergence of physical and non-physical domains and that non-physical domains, such as cyber and the pervasive information environment constitute new challenges for warfighting thus leading to a multi-dimensional battlespace: physical, virtual, and cognitive. The NWCC aims to put the Alliance in a position to out-think, out-excel, out-fight, out-pace, out-partner, and out-

[3] Department of Defense, Office of the Director of National Intelligence (2011) National Security Space Strategy Unclassified Summary. Washington DC, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

last any threat or challenge. This will be reflected in new, cohesive concepts across all operational domains in order to be effective within the multi-dimensional battlespace in order to maintaining decisive advantage against any adversary with space as a critical operational domain.

The NWCC hast set out five Warfare Development Imperatives: cognitive superiority, layered resilience, influence, and power projection, integrated multi-domain defence, and cross-domain command. Clearly, space systems offer significant contributions throughout the spectrum of Warfighting Imperatives. The growing capabilities of space in fields such as remote sensing, navigation, positioning and timing and communications will bring a vast array of applications and services that impact NATO members' societies and will become embedded in economy, security, and administration. Space systems will serve an important coordinating role and, in time, they may serve as the upper layer of command and control for all infrastructure systems.

A new EU space strategy for security and defence will be developed by the end of 2023., Here we can also expect that space will be considered as a major key to success. Vis-à-vis an increasingly growing dependence on space resources and the “weaponisation" of space by strategic competitors, EU focus will likely be on:

- Investment in SSA and space-based Earth observation, critical space technologies, developing capabilities to ensure autonomous EU access to space;
- strengthened dual-use innovation;
- better protection of space supply chains;
- exercises aiming to improve the resilience of space assets and address vulnerabilities in order to respond quickly and decisively to space-related threats;
- expansion of the EU space program;
- deepen political dialogue and cooperation with NATO in space-related matters.

As the EU needs secure and resilient global connectivity, it aims at:

- global satellite communication coverage for dual-use purposes which is increasingly handled as strategic infrastructure;
- secure connectivity;
- strategic autonomy and new industrial alliances, including on secure telecommunication networks;
- synergies between civil, defence and space industries aimed at establishing an EU Space-based Global Secure Connectivity project;
- completing the EU’s space capacity, along with the EU’s satellite navigation and Earth-observation systems, Galileo and Copernicus;
- advanced connectivity capabilities and innovative quantum technology;
- supporting the GovSatCom approach;
- synergies with all the EU space programme components.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

6. Perspectives

NATO and EU evolutions take place in the context of a heating up of competition in space in parallel with an evolving panoply of threats to space systems, which have also become accessible to non-governmental actors. The recent years saw anti-satellite weapons tests from China (2007 and 2014) and India (2019). Various risks to space systems are increasing and can harm Western security and commercial interests. Some countries, including Russia and China, have developed and tested a wide range of counter-space technologies that could restrict Western access and freedom to operate in space.

Against this backdrop we can expect both NATO and the EU to define collective positions, approaches, systems, and tools to protect their interests in space, both as a continuing factor in growth, prosperity and innovation, but also to secure it in a complex, dynamic and worsening security environment.

***

Remarks: The opinions expressed in this contribution are those of the author.

About the Author of this Issue

Ralph D. Thiele, retired Colonel, is President of EuroDefense (Germany), Chairman of the Berlin-based Political-Military Society, and Managing Director at StratByrd Consulting. In his 40-year military career in the German Armed Forces, he has held key national and international positions. He also offers advice in his honorary and business functions on defence innovation in times of digital transformation. He has most recently published the book “Hybrid Warfare. Future and Technologies.”

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de