Ralph Thiele

AUSTRIA INSTITUT FÜR EUROPA- UND SICHERHEITSPOLITIK

Special Series on the Strategic Review of Global Hotspots

FOKUS | 6/2021

Space Competition

This special Fokus series on the Strategic Review of Global Hotspots consists of seven parts and is based on the AIES online discussion on the same topic. The online lectures of the authors are available at: aies.at/global-hotspots

1. Context

Geostrategic competition is global in scope. The boundaries between civil and military competition have become fluid and marked by geostrategic competition, multiple hybrid threat situations, attacks on businesses and critical infrastructure, and the threat of prolonged, low-intensity or shorter, high-intensity conflicts.[1] Hybrid scenarios are gaining in importance as a preferred form of confrontation.[2]

In particular, Russia and China integrate civil and military competition at every level, including the development of their international trade, investment, national technology base, and political and diplomatic activities. Both are using new, disruptive dual-use technologies as the key to advancing own capabilities and geopolitical ambitions. The dynamics of this geostrategic environment present EU, NATO and member states with a variety of demanding requirements. In this equation space holds a critical role.

Space-based services have become key to commercial, governmental and military systems, platforms and information requirements. Space systems imagery, and geolocation services allow users to access and fuse data and information in near real-time. Together with timing and navigation, space-based capabilities provide secure high bandwidth and the connection of fixed and on-the-move 5G networks.[3] They enable high mobility, wide geographical coverage and precision. In particular, military command & control use space-based systems, coupled with meshed networks systems to support deployed operations as these enable data-exchange in difficult environments. The use of space and space-derived data will likely increase over the next two decades.

2. Open for Business

For half a century, space-related innovation meant scaling Apollo-era technologies. Ever larger, weightier, billion-dollar satellites were designed to operate for forty years or more. Participation in such projects was reserved for a few, elite organizations and large corporations. Governments and military leaders set the direction and provided large budgets.

Today, seventy-five percent of space revenues are earned commercially.[4] As access to space gets cheaper, satellites are becoming mass-produced devices. Evolving technologies have brought space capability into the reach of states, international organisations, corporations and individuals that a decade ago had no realistic ambitions in this regard. In between, more than 80 countries have entered the global space industry. Ongoing technological progress is a key catalyst.

For example, miniaturization allows the development of smaller launch vehicles, which in turn can spend comparatively small and light satellites with enhanced capabilities. Thanks to breakthroughs in modular computer architectures, robotics, artificial intelligence and more, new launch systems and satellites are becoming cheaper, more innovative and more useful. Commercial space companies have stimulated innovation with new business models and the integration of disruptive technologies.[5] Space applications are both a prerequisite and an important driver for future technologies such as 5G, additive manufacturing, autonomous systems, IoT and many others.

Currently, an almost revolutionary variety of satellites are taking off into space, especially low- and medium-orbit, digital-capable, largely interference-resistant, highly flexible in operation, with enormous bandwidths and low latency. SpaceX's Starlink program in particular shows how it's done. Every month Elon Musk is currently putting up to 60 Starlink satellites into orbit simultaneously per launch with his Falcon 9 launch system – already 955 in total by the end of 2020. The current license is for 12,000 satellites in low orbit. The application for another 30,000 has been filed. OneWeb and Kuiper (Amazon) are planning on a comparable scale.

Satellite communications have fuelled the majority of commercial growth since the 1980s. This development will also drive progress as regards government and defence usage in the upcoming decade as their demand for satellite communications is constantly increasing – from a level of approximately 35Gbps today to a projected 150Gbps and more by 2025.[6] Additionally, there is the rapidly growing global demand for earth observation data and the increasing demand for highly accurate satellite navigation systems providing significant potential for the development of new products and services. Both, large companies and start-ups have been investing in space as a promising business sector.

3. No Fence in Space

Serious threats to space infrastructure are relatively new phenomena. For a long time, space used to be an ecosystem of its own. As more countries and commercial firms have begun participating in satellite construction, space launch, space exploration, and so forth, new risks and threats have also emerged for space-enabled services. In this widening battlespace of the future, it will be much harder for EU, NATO, member nations and allies to defend against every possible threat given asymmetry of the possible attacks and the diversity and complexity of the attack vectors. Today, it is increasingly understood that space assets have been vulnerable to all kind of attacks for far too long.

The taxonomy of space weapons developed by Todd Harrison provides a well-structure overview of the developing threat spectrum: [7]

- ★ Earth-to-space kinetic, include physical systems such as anti-satellite (ASAT) missiles designed to destroy satellites without placing the weapon system or any of its components into orbit.
- ★ Earth-to-space non-kinetic, includes jammers, laser dazzlers or cyberattacks launched from Earth aiming to interfere, temporarily or permanently, with satellite capability.
- ★ Space-to-space kinetic, includes physical systems launched from other satellites physically intercepting satellites in order to disrupt or destroy them.
- ★ Space-to-space non-kinetic, includes disrupting space-based systems from another satellite using non-kinetic means such as high-powered microwaves, jammers, and robotic technology for satellite servicing and repair.[8]
- ★ Space-to-Earth kinetic, addresses impacting a terrestrial target from space.
- ★ Space-to-Earth non-kinetic, addresses impacting terrestrial targets by lasers, high-power microwaves, and other types of radiofrequency weapons.

All of these systems exist – perhaps with the exception of space-to-earth kinetic as there is no confirmed open knowledge. They are tested by several actors from East, West and elsewhere. We can expect upcoming capabilities for manoeuvre warfare in space.

With battlefields being heavily impacted by disruptive technologies and warfare becoming increasingly hybrid, an array of disrupting technologies is spilling over into the military domain, including robotics, energy storage solutions, cloud computing, advanced materials, nano technology, 3D printing and many more. Many of these disruptive technologies that are relevant for the military originate from the commercial sector. As a consequence, the number of vulnerabilities keeps further growing.

Along with the masses of small satellites that have started populating space in the future, space debris will increase rapidly. Given their enormous speed, even very small objects can cause a huge amount of damage. The risk of collision with debris – akin to that of being hit by an ASAT missile – magnifies the already existing problem of congestion in space, thus rendering orbits unusable. Against this backdrop, the capability of Space Situational Awareness (SSA) has gained in relevance in order to deliver detailed knowledge of any given space object's location, and to ensure the ability to track and predict its future location.

Of course, cyber threats have an important role in space. Actors can use offensive cyberspace capabilities and other hybrid means to enable a range of reversible to non-reversible effects against space systems. In particular, hybrid warfare allows for the diffusion of opponents' SSA via information operations, i.e. electronic warfare, and cyber operations. In fact, upcoming challenges cross-cut space and cyber domains. Ground-based space infrastructure is particular vulnerable to cyber-attacks. There are plenty of access points which can be attacked – including the antennae on the satellites, the ground stations, and the earth-based user terminals. Such attacks range from exploiting the physical vulnerabilities of a ground site to electronic warfare, to disrupting the connection between the space segment and the operator.

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

4. Space Race

Vis-à-vis these challenges, the unhindered access to – and freedom to operate in – space has become of vital importance to NATO, the EU and their member nations.[9] Their military strength rests in large part on space-based C4ISR[10], timing and navigation. Competitors and opponents understand this. Space has long been their focus of attack to weaken Western command and information systems. Emerging quantum technologies - including space-based sensors and secure communications and data processing based on quantum encryption – will add to the existing trend.

NATO has only recently discovered space as an operational domain, though it has built own C4ISR capabilities decades ago, on a predominantly US backbone. NATO's Secretary General Jens Stoltenberg stated in late 2019,

"Making space an operational domain will help us ensure all aspects are taken into account to ensure the success of our missions …". [11]

In Europe, in the past, three flagship programmes – Copernicus, Galileo, Egnos – have been at the fore of its space activities. With view to upcoming challenges the EU also strives for high-quality, and secure space-related data and services as well as a leading role for the EU in the space sector.[12] Current initiatives aim to strengthen capabilities with view to critical infrastructures, cyber-security or quantum technologies.[13] Governmental Satellite Communications (GOVSATCOM) as another key space initiative of the EU at the crossroads of space, security and defence aims to ensure reliable, secure and cost-effective satellite communication services in both the commercial and military environments.

The US is focussed on maintaining leadership in space as it considers space as of vital national interest. In December 2019, the US Congress authorised building the United States Space Force. Its mission will be to:

- ★ run the existing constellation of US military satellites that are currently managed by the services;
- ★ operate the military's launch facilities;
- ★ execute financial planning and programming to purchase satellites and ground support equipment; and
- ★ train a specialised cadre of space officers and enlisted personnel.[14]

Also, 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 allies, and have implemented this goal by means of military reorganisation in 2015. Both countries have developed robust and efficient capabilities, including space-based ISR, as well as improvements to space launchers and satellite navigation constellations. These provide for monitoring opponents forces and deploying own forces in a targeted manner.

China has expanded its space capabilities by several orders of magnitude. The scale of Chinese investment surpasses that of all other nations. China is the lead rocket-launch nation in the world. It operates two space stations, and has only recently landed a lunar rover on the far side of the moon. In 2018, the country conducted 25 per cent more orbital launches than the US. Counterspace capabilities are of particular interest to China. In 2018 alone, it tested several ASAT.

Long gone is the Soviet Union's Cold War era dominance in the space domain. Yet, Russia remains a prominent space power. Since the mid-2000s, Russia has started modernising many of its languishing space capabilities. It appears that it is currently developing ASAT weapons, ground- and air-based laser weapons, and a network of electronic weapons, supported by capable offensive cyber capabilities, targeting satellite systems and related ground stations.

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 ASAT missiles. Russian and Chinese satellites have repeatedly demonstrated their capabilities for precise maneuvers in space. These enable, for example, the repair of satellites in space, but also provide the capability to damage or destroy satellites of opponents without kinetic impact.[15]

Focus and investment

The more space is used for security purposes, the more infrastructures and services must be secure and reliable.[16] Consequently, the EU aims to translate the upcoming hybrid and disruptive technological challenges into viable, security/defence capabilities, which also yield dividends on both European and global markets. This calls for an orchestrated, focussed and engaged investment in research & development in order to ensure that innovation responds to commercial and military needs, but also enhances the capacity to manage space technologies and protect critical space infrastructures.

At a time where Industry 4.0 is revolutionising collaboration, production and services, integration of satellite Internet of Things (IoT) and Global Navigation Satellite System (GNSS) constitute a valuable capability to loop hardware products in both remote and extreme environments.[17] Already today, there is a premium on disruptive and game-changing technologies that are autonomous, reconfigurable, agile and adaptable. The space industry benefits in particular from advanced technologies, capabilities, business models and services. These include:

- ★ Real-time, multi-domain Space Situational Awareness;
- ★ Automated cyber forensics and analytics;
- ★ Autonomous and automated space systems;
- ★ Digital beam forming, able to reconfigure SAT footprints as missions require;
- ★ On-board resilience and self-healing satellites;
- ★ New concepts in space-ground operations, i.e. enhanced predictive technologies, or dynamic encryption;
- ★ Hardware products, such as flat panel antennas (FPA), that will increase the efficiency of satellite communication on-the-move demand for armed forces;
- ★ Predictive and automated threat analysis, advanced data analytics;
- ★ Advanced quantum capabilities in the areas of computing and cryptography.

NATO, the EU and their respective member nations would be well-advised to further increase their investment in space-related research and development (R&D) activities. Innovation needs to be upscaled, taking advantage of disruptive technologies such as AI, robotics, 5G or quantum for space capabilities. Not only the commercial competition in space is challenging. Hybrid and further threats to security and defence are real and growing dynamically.

Ralph Thiele, President, EuroDefense Germany and Managing Director, StratByrd Consulting.

Endnotes

1) Ralph Thiele. Disruptive Technologien - Chancen und Risiken im Kontext hybrider Gefahrenlagen. In Jäger, Thomas, Daun, Anna, Freudenberg, Dirk (Hrsg.). „Politisches Krisenmanagement 3: Führung, Recht, Organisationen". 2021.
2) Anthony Cordesman. The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy. CSIS 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/2020811.Burke_Chair.AHC_.GH9_.pdf
3) Matt Leonard. Encrypting satellite communications. GCN. 27 April 2018. https://gcn.com/articles/2018/04/27/darpa-satellite-communications-encryption.aspx
4) Wilbur Ross. Remarks at the Sixth National Space Council Meeting. U.S. Department of Commerce. Washington, Tuesday, August 20, 2019. https://www.commerce.gov/news/speeches/2019/08/remarks-us-commerce-secretary-wilbur-l-ross-sixth-national-space-council
5) ESRE. Whitepaper. Selected Trends and Space Technologies Expected to Shape the Next Decade. November 2017. https://esre-space.org/wp-content/uploads/2018/01/ESRE_Whitepaper_-2017.pdf
6) Patrick Biewer. The future of secure satellite communications. Luxembourg Space Agency. 13 December 2019. https://space-agency.public.lu/en/news-media/news/2019/the_future_of_secure_satellite_communications.html#
7) Todd Harrison. International Perspectives on Space Weapons. May 2020. https://aerospace.csis.org/international-perspectives-on-space-weapons/
8) DIA. Challenges to Security in Space. January 2019. https://www.dia.mil/News/Articles/Article-View/Article/1754150/defense-intelligence-agency-releases-report-on-challenges-to-us-security-in-spa/
9) EDA. 2018 CDP Revision. The EU Capability Development Priorities. Brussels. Pg. 9. https://www.eda.europa.eu/docs/default-source/eda-publications/eda-brochure-cdp
10) Command, Control. Communication, Computer, Intelligence, Surveillance, Reconnaissance
11) Daniel Boffey. NATO leader identifies space as the next 'operational domain'. Brussels. November 20, 2019. https://amp-theguardian-com.cdn.ampproject.org/c/s/amp.theguardian.com/world/2019/nov/20/nato-identifies-space-as-next-operational-domain
12) Council of the EU. The EU shapes its future space policy programme. Brussels. 13 March 2019. https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/eu-shapes-its-future-space-policy-programme/
13) UKRI. UK and Singapore collaborate on GBP 10m satellite project. 27 September 2018. https://stfc.ukri.org/news/uk-and-singapore-collaborate-on-10m-satellite-project/
14) James Stavridis. Space command - What to expect when you're expecting a new branch of the military. Bloomberg News (TNS) December 30, 2019 http://m.startribune.com/what-to-

expect-when-you-re-expecting-a-new-branch-of-the-military/566569632/

15) DIA. Challenges to Security in Space. January 2019. https://www.dia.mil/News/Articles/Article-View/Article/1754150/defense-intelligence-agency-releases-report-on-challenges-to-us-security-in-spa/

16) Kai-Uwe Schrogl (Editor in Chief). Handbook of Space Security 2020 (2nd edition). Berlin 2020. https://www.springer.com/gp/book/9783030232092

17) Juan Fraire, Sandra Céspedes, Nicola Accettura. Direct-To-Satellite IoT - A Survey of the State of the Art and Future Research Perspectives: Backhauling the IoT Through LEO Satellites. ADHOC-NOW2019: Ad-Hoc, Mobile, and Wireless Networks, Oct 2019, Luxembourg, Luxembourg. pp.241-258, 10.1007/978-3-030-31831-4_17. hal-02315399 https://hal.laas.fr/hal-02315399/document

Dr. Langweg 3, 2410 Hainburg/Donau
Tel. +43 (1) 3583080
E-Mail: office@aies.at
Website: www.aies.at

Layout: Medienbüro Meyer