Version 1.1

Recent Trends in the Space Security Environment – yearly update

EURODEFENSE SPACE OBSERVATORY

Under the cover of the media impact of events such as the Russian invasion of Ukraine, or the continuing effects of the resurgent pandemic in China and elsewhere, a quiet structural shift is underway with regards to the space and the powers marshalling resources to explore and exploit it. This new Space Race involves not only state actors, but also non-state actors, primarily corporations, and features not only a scientific, civilian and economic dimensions, but also a security and military one.

The following information and conclusions were drawn from an analysis of space-related reports appearing in 2021 and 2022, as well as other open-source intelligence sources.

Table 1. Open-source satellite number database with key statistics (source: UCS, 2022)[1]

Satellite Quick Facts *(includes launches through **29.12.2021**)*			
Total number of operating satellites: 4,852			
United States: 2,944	Russia: 169	China: 499	Other: 1,240
LEO: 4,078	MEO: 141	Elliptical: 59	GEO: 574
Total number of US satellites: 2,944			
Civil: 30	Commercial: 2,516	Government: 168	Military: 230

These are the most important overall structural trends in space:

- The diminishing launch costs;
- The standardization of satellite platforms, with satellites based on these platforms becoming the vast majority of non-governmental satellites in orbit[2];
- The continuing miniaturization of satellite components;
- The entry of new players, both state and non-state into space;
- The rise of mega-constellation owners, such as Starlink and OneWeb;

[1] Union of Concerned Scientists (2022). Open-source satellite database. https://www.ucsusa.org/resources/satellite-database

[2] Bryce Aerospace (2022). Smallsats by the numbers 2022. https://brycetech.com/reports/report-documents/Bryce_Smallsats_2022.pdf

- The rise of New Space start-up sector, as a locus for technological innovation and the fast growth in the number of space-enabled products and services;
- The continuing erosion of norms against the militarization of space. Continued testing of ASAT weapons and non-destructive systems with ASAT potential such as maneuvering satellites indicate a preparation phase in anticipation of the first overt attacks on space infrastructure. The use of SpaceX Starlink satellites to provide Internet connectivity to areas of Ukraine intentionally cut off from physical network infrastructure has led to threats on the part of Russia against these systems. The reply of the CEO of SpaceX has been that the company possesses the capability to replace these systems faster than any player can destroy them.

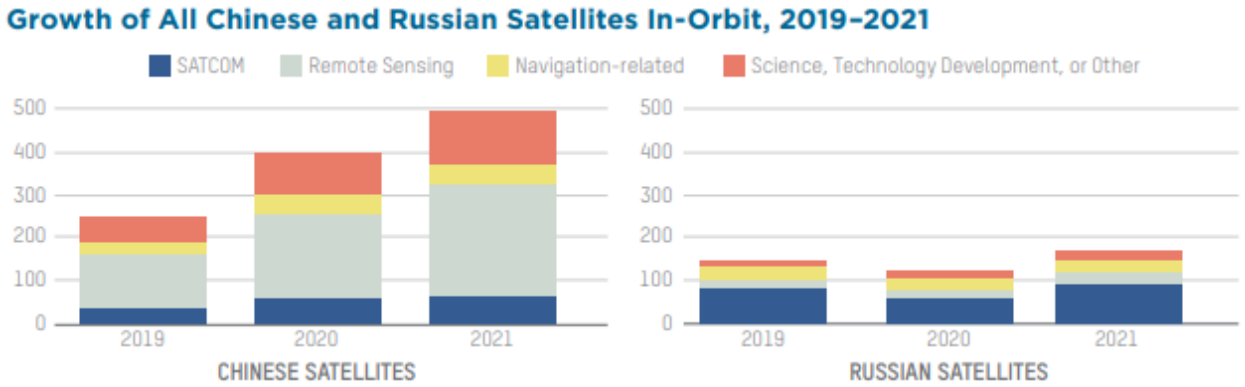

Figure 1. Growth of Chinese and Russian satellite inventories 2019-2021 (source: DIA, 2022)[3]

Key developments in capabilities for China:

- In 2021, China conducted 52 successful launches, three failed launches and supposedly tested a hypersonic glide vehicle;
- In May 2021, China became the second country to land and maneuver a rover on Mars, Zhuhong;
- China's 2016 white paper on space states the goal for "To build China into a space power in all respects."[4];
- The 2021 white paper stresses also military development and the development of a private domestic space industry to lessen the reliance on imports from international markets and companies. This vision is why China lifted its ban in 2014 on private space sector companies[5];

[3] Defense Intelligence Agency (2022). 2022 Challenges to Security in Space. Washington DC. USA, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

[4] "Full Text of White Paper on China's Space Activities in 2016," State Council, People's Republic of China, December 28, 2016, http://english.www.gov.cn/archive/white_paper/2016/12/28/content_281475527159496.htm

[5] Harrison et al. (2022). Space Threat Assessment Report 2022. Center for Strategic and International Studies, Washington, US, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220404_Harrison_SpaceThreatAssessment2022.pdf?K4A9o_D9NmYG2Gv98PxNigLxS4oYpHRa

- China started awarding contracts in 2021 to build a new launch site in Ningbo, which will be able to host 100 launches per year when done, compared to the 55 launches China had on the whole in 2021. China is also building a sea-based launch platform;
- China launched a space cooperation framework in 2019, as the Belt and Road Initiative Space Information Corridor. The 2021 White Paper highlights successes in Egypt, Pakistan and Nigeria, when it comes to satellite research and infrastructure building.

Key developments in capabilities for Russia:

- A fourth test flight of the new Angara A5 heavy lift vehicle is scheduled for 2022, after the previous one failed to insert into orbit due to an engine malfunction. It will be capable of reaching LEO and GEO;
- The Vostochny Cosmodrome in Eastern Russia is undergoing construction. It is already launching Soyuz 2 rockets. It will replace the Baikonur Cosmodrome in increasingly unstable Kazakhstan;
- "Russia possesses counterspace weapons in all four categories: kinetic physical, non-kinetic physical, electronic, and cyber"[6];
- Russia tested a new ASAT system, A-235 PL-19 Nudol, which is a ballistic anti-missile and anti-satellite system, in November 2021, from the smaller Plesetsk Cosmodrome;
- Russia has proven the capability to have satellites that "nest" inside one another and then separate in space, as well as the ability to perform RPOs and to synchronize orbits with other satellites. The Luch geostationary satellite launched in 2014 continues to shift its position even now, getting close to satellites from other nations;
- In February 2022, the director of the US National Reconnaissance Office, Christopher Scolese, warned satellite operators to "ensure that your systems are secure and that you're watching them very closely because we know that the Russians are effective cyber actors."[7]
- Russia added to its SIGINT capabilities by launching two more satellites in 2021 for the Liana constellation and by building the Sledopyt ground system to intercept radio communications from satellites orbiting above Russian territory;
- Russia has consistently utilized GPS jammers and other counterspace capabilities in the region of Ukraine, both to hinder Ukrainian forces and outside actors, including OSCE drone monitoring missions.

[6] Ibidem

[7] Sandra Erwin, "NRO warns satellite operators of possible Russian attacks," SpaceNews, February 23, 2022, https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-asukraine-crisis-unfolds/

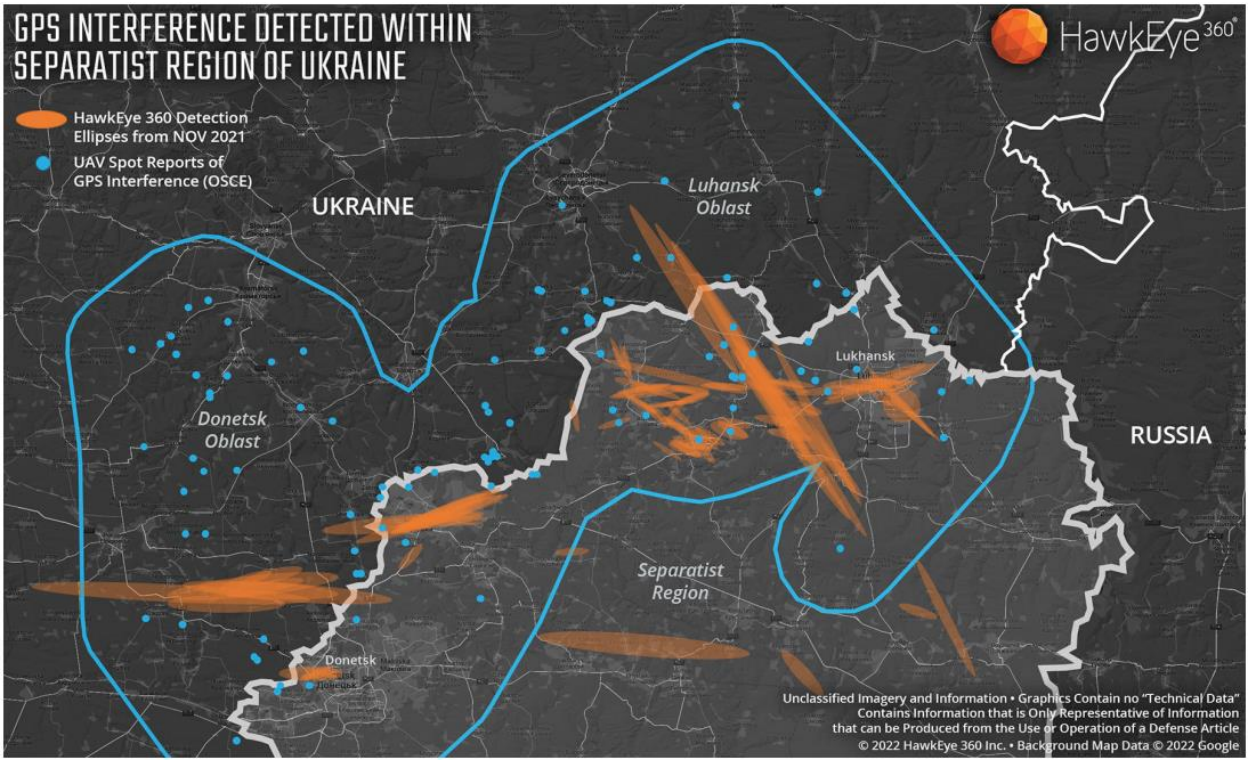

Figure 1. Map of GPS interference in the disputed Donbas region, prior to invasion (source: CSIS, 2022)

Key developments in capabilities for India:

- The Indian Space Research Organization is the sixth-largest space agency in the world, operating under the Department of Space directly under the Prime Minister;
- India founded a Defence Space Agency in 2019 through the merger of the Defence Imagery Processing and Analysis Centre and the Defence Satellite Control Centre. It has few published materials, but India's Defence Research and Development Organisation has been advocating for "hypersonic launch vehicle [sic], small Inter Continental Ballistic Missiles, and ASAT capability with capacity to strike both LEO and Geosynchronous Orbit (GEO)"[8];
- India has been investing heavily in military intelligence satellites;
- In October 2021, Prime Minister Narendra Modi launched the Indian Space Association to foster public-private ties in space;
- India performed its own ASAT test in 2019, and the system "has the capability to neutralise the target satellites in the entire LEO region"[9];
- Due to its longstanding security and defence cooperation with Russia, India was silent during the condemnation of Russia's tests in 2021;

[8] Namrata Goswami (2022). Indian Space Program and its Drivers: Possible Implications for the Global Space Market (Paris: IFRI, European Space Governance Initiative, January 2022), 16, https://www.ifri.org/sites/default/files/atoms/files/goswami_indian_space_program_2022_.pdf

[9] Dinakar Peri (2021). "Two years since ASAT test, DRDO working on several key space technologies". The Hindu, March 26, 2021, https://www.thehindu.com/news/national/two-years-since-asat-test-drdoworking-on-several-key-space-technologies/article34171447.ece

- "India has demonstrated a successful kinetic direct-ascent ASAT capability, but there have been no public reports confirming non-kinetic capabilities. India has developed electronic warfare systems on the ground and has demonstrated cyber proficiency, though it not clear if India targets space systems in its electronic or cyber systems"[10].

Other countries with significant space and ASAT potential now and in the future, aside from the US, include North Korea, Iran, Israel, Japan and South Korea.

Noted counterspace activities in 2021, according to the CSIS[11]:

- Constant reports of jamming of radio, cell, and satellite signals in Ukraine;
- Commercial jammers that look like everyday objects identified in China, including jewelry and USB sticks (12 March 2021, China);
- GPS jamming of OSCE mission utilizing UAVs in Ukraine to monitor Russian build-up (6 April 2021, Russia);
- China's GEO inspector satellite SJ-17 reported to have a robotic arm onboard, which had not previously been disclosed. The satellite has RPO capabilities, meaning it can match orbits and velocities with other satellites (20 April 2021, China);
- Cyprus-flagged oil tanker Berlina spoofed its own GPS-backed automatic identification system (AIS) signal in order to evade sanctions and transport illegal oil from Venezuela (28 May 2021);
- The GPS systems of a UK Royal Navy destroyer and a Dutch Royal Navy ship moored in Odessa during a NATO mission were falsified via spoofing to appear to be in Crimea (17 June 2021, Russia);
- A US Navy destroyer was spoofed to appear to be near Crimea rather than near Ukrainian held waters (30 June 2021, Russia);
- Possible hypersonic test by China (28 July 2021, China);
- Australia announces Project 9358, an electronic warfare project (29 July 2021, Australia);
- Instructions for GPS spoofing found online (25 September 2021);
- Chinese scientists publish research results from a government funded project on how an explosive device could be placed on an enemy satellite via another satellite. The paper was published in the Journal of Electronic Technology and Software Engineering, published by the Chinese Association for Science and Technology and the Chinese Institute of Electronics (23 October 2021, China);
- Chinese satellite SJ-21 launched in October 2021 performed exercises in orbital positioning with another unidentified system (01 November 2021, China);
- Russian live fire test in LEO of a ground-based kinetic physical direct-ascent ASAT weapon, the Nudol System, against an inactive Soviet satellite (15 November 2021, Russia);
- New facilities for electronic warfare built on Hainan Island (21 November 2021, China);
- Russian officials indicated in a TV broadcast that Russia can target and destroy all 32 US GPS satellites (29 November 2021, Russia);
- Russian S-550 missile entered combat duty in December 2020. It could be used against satellites (29 December 2021, Russia);

[10] Idem 3
[11] Idem 3

- An undersea cable between Norway and the Svalbard archipelago was severed. The state company Space Norway AS maintains the fiber-optic cable and operates the Svalbard Satellite Station. There was redundancy in place and the cable was repaired by 21 January 2022 (7 January 2022);
- Suspected hack of Viasat ground terminals in Eastern Europe, including Ukraine, on the day of the Russian invasion (24 February 2022).

Conclusions for Europe:

- The growing importance of space to national and collective security;
- The use of counterspace capabilities not only for state interests, but also to enable private and non-state criminal activity, increasing the fragility of space systems and the vulnerabilities inherent in their use;
- The increased vulnerability of space systems. They are vulnerable not only to direct threats, but also as third-party casualties to the confrontation between other space actors, through debris creation, jamming and other phenomena. Given the interconnections between space services use at global level, one actor attacking another may decide to strike against third party satellites to further degrade the space capabilities of the intended target;
- The importance of the private sector for space development, as a source of funding, expertise and RDI potential;
- The erosion of norms against the militarization of space and its maintenance as free to access for all mankind for peaceful purposes;
- Europe is falling behind other actors in the new Space Race. It has neither the focused capabilities and resource mobilization potential of China, the private sector dynamism and entrepreneurialism of the United States or the geopolitical or security focus of the Russian Federation.

From 10 to 13 May, the EU carried out the Space Threat Response Architecture (STRA-22) exercise in the European External Action Service Headquarters in Brussels. The Space Threat Response Architecture Exercise (STRA-22) is the fourth exercise of its kind and was organized by the EEAS, together with the Commission and the EU Space Programme Agency (EUSPA). This exercise tested the EU´s response capacity to a situation in which an EU space asset is subject of an attack targeting essential or critical services. These situations can take various forms: an attack on a satellite, space debris threatening civilian populations, cyber-attacks, spoofing or jamming satellite signals.

The exercise activated the EU´s response mechanisms and involved all relevant political, diplomatic and technical actors to be mobilized in such situations, from the Galileo Security Monitoring Centre (GSMC) to the High Representative and the Council.

Governments, businesses and citizens rely on space-based assets and services for the functioning of their economies and activities, as well as for security and defence.

As part of the Strategic Compass, the EU is redoubling efforts to be better prepared to respond to threats in space. By 2023, the High Representative and the Commission will present an EU Space Strategy for Security and Defence. The exercise will feed into this reflection, nurturing a common strategic approach to these issues.

Recommendations for Europe:

- Europe should define and build a space strategic culture that accentuates its strengths, minimizes its weaknesses and articulates and justifies its goals to the world and to itself. This is an important counterpoint to the various strategic documents and other proposals which have been launched;
- While not militarizing per se, Europe should consider securitizing its space projects, starting with considering their utility for security, their impact on security and their requirements for security, in addition to the already included economic, environmental and social dimensions. The GOVSATCOM project is the first European space project with an explicit security focus, since it proposes to establish secure satellite communications for European governments. Future projects should also be selected in accordance with requirements for strategic autonomy and strategic technological autonomy, including with an overarching security focus;
- While Europe may not militarize, its individual Member States have been exploring the military dimension of space, by creating Space Force equivalents and possibly conducting research into counterspace capabilities and protection measures. The European Union should set up a Space Security Board as part of the Council on Space and working in close connection with DG-DEFIS to enable information sharing on these capabilities and conducts a European Space Defence Review as a part of evolving European Defence initiatives and capabilities.
- Cooperation between the EU and NATO on space should also be considered a priority. NATO does not have its own space assets and is reliant on information and asset sharing between MS for defence purposes. The EU's significant space asset base can be included in a way which is more difficult for the individual NATO and EU Member States acting on their own initiative. As an example, taking advantage militarily of Galileo receiver station compatibility with GPS can increase battlefield resilience. The EU can also prioritize polar-orbit satellites for environmental studies that can also be used to cover gaps in NATO polar space capabilities. This would add a space dimension to an already burgeoning cooperation between the EU and NATO, which includes cyber, maritime and hybrid threats dimensions. Their cooperation will likely lead to the linking of their likely space operational security and awareness centers (on the basis of the NCIRC and EU-CSIRT cooperation model) that will integrate Space Situational Awareness information streams from civilian efforts;
- Europe should focus on mobilizing its private sector resources and its entrepreneurialism to act as a multiplier to state-led investment into space. Europe has far fewer private investors into space start-ups than either the US, China and the UK[12]. Interviews with industry participants highlighted that the problem is not just lower start-up creation levels, but also lower start-up survival levels, implying a lack of state support for the advancement of ideas beyond the critical initial phase, lack of access to relevant infrastructure (often state-owned), but also (and especially) a lack of private sector appetite for risk related to space enterprise;

[12] Bryce Aerospace (2022). Start-Up Space Report 2022. https://brycetech.com/reports/report-documents/Bryce_Start_Up_Space_2022.pdf

- A potential approach towards stimulating the involvement of the private sector into space is to copy the EU approach for the InvestEU Programme 2021-2027[13], which has a security dimension related to cyber and AI, among others. InvestEU targets 650 billion euros in the 2021-2027 timeframe, divided thusly: 15,2 bln from the European Commission, 38 bln from Member States, of which 11.8 bln are dedicated to research, and 9.5 bln from various partners. The rest is external contribution, meant to be attracted mostly from the private sector as a result of state and EU-led investment, with a multiplier of 13.8. Whether feasible or not in the required timeframe, the InvestEU model consciously approaches the issue of multiplying the public-sourced investment by attracting private investment, and can serve as a model for future space development;
- The European Union should aim to employ the "Brussels Effect" to delay the militarization of space and the onset of space conflict, until it has closed the capability gap with its main systemic rivals. The Brussels Effect refers to the EU's capability to set norms, rules and standards that are followed by entities outside the EU's borders, and is a key component of European soft power. However, fostering a Brussels Effect in any advanced technology domain requires that the EU itself become a (aspiring) leading player in that field, whether we are talking about AI[14] or space. The EU should focus on preventing conflict in space, developing norms regarding the registration of space assets, norms regarding the assignment of liability for space disasters and damage done by debris, and norms/treaties regarding the prevention of cyber-attacks, jamming and spoofing;
- Provide support to Member States to organize Space Threat Response Architecture Exercises (the European variant of the French ASTER exercises) or various evaluations at national levels to increase awareness of critical dependence on space services and technologies;
- Begin developing dual-use technologies in space, including debris clean-up and mitigation technologies.

[13] European Commission (2019), InvestEU Programme, https://ec.europa.eu/commission/sites/beta-political/files/what_is_investeu_mff_032019.pdf

[14] Erik Brattberg, Raluca Csernatoni, Venesa Rugova (2020). Europe and AI: Leading, Lagging Behind, or Carving Its Own Way? Carnegie Endowment, 9 July 2020, https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236