Hybrid CoE Working Paper 21

The space domain and the Russo-Ukrainian war: Actors, tools, and impact

Hybrid CoE

Marko Höyhtyä and Sari Uusipaavalniemi –
January 2023

Hybrid CoE Working Papers cover work in progress: they develop and share ideas on Hybrid CoE's ongoing research/workstrand themes or analyze actors, events or concepts that are relevant from the point of view of hybrid threats. They cover a wide range of topics related to the constantly evolving security environment.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

ISBN 978–952–7472–52–1 (web)
ISBN 978–952–7472–53–8 (print)
ISSN 2670–160X (web)
ISSN 2814–7235 (print)

January 2023

Cover photo: Andrey Armyagov / shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Summary

This Hybrid CoE Working Paper discusses how the space domain has been used and impacted during the ongoing war in Ukraine. The space domain has arguably not been used in such a versatile manner in any previous conflict, duly providing a major learning opportunity for Western countries. The focus of this paper is on hybrid threats, tools and actors, and it provides a comprehensive analysis of achieved and predicted impacts, including linkages between the space domain and other hybrid threat domains. Attacks on and hybrid threats towards space infrastructure can have very wide-scale effects since modern societies rely heavily on space-based capabilities. For example, systematic cyberattacks against satellite systems can prevent information sharing and cause disruptions to the energy and transportation sector. There are several lessons learned: 1) The power of crowdsourced situational awareness has been demonstrated in the war. Information from the civilian population has been used to support operations in the field. 2) The Russo-Ukrainian war has paved the way for satellite-based technologies to turn into easily accessible everyday tools for both the military and the civilian population. The war has proved that owning space capabilities is not as crucial as having access to them, as shown by the review of some of the most important commercial actors and how their services have been used during the conflict. 3) The use of commercial space assets in military operations is blurring the line between military and civilian actors in the war. 4) Developments in satellite technologies and their use also foster new combinations of capabilities that can be used for military purposes. A major threat caused by the war to the space environment and substantial international space programmes has been the degradation of the cooperative spirit among countries. A clear consequence of this are the increasing efforts to ensure sovereignty through each country's own national or regional activities.

Introduction

Russia's war against Ukraine since 24 February 2022 has been described as the first 'two-sided space war'.[1] The space domain has been used in an ever more agile and flexible way with links to other hybrid threat domains. In particular, the importance of commercial and private resources in utilizing the space domain has been highlighted, and international space cooperation has experienced major setbacks due to the war. China and Russia are developing anti-satellite capabilities along with electronic and cyber weapons,[2] while Western states are re-assessing their security priorities and developing space strategies. Evolving space threats, new space phenomena, dual-use capabilities, and the increasing criticality of space-based capabilities to societies' vital functions shape the partnerships and collaboration in the space domain. At the same time, the current global space governance framework is inadequate and ineffective in managing space activities and security in space.[3] This leaves opportunities for hybrid actions and complicates the pursuit of coherent countermeasures in space.

Hybrid threats can be defined as coordinated and synchronized actions that deliberately target the systemic vulnerabilities of democratic states or institutions in order to reach strategic goals and create the desired effects. Actions are usually carried out in multiple domains, and the hostile actor can also aim at creating completely new vulnerabilities.[4] The space domain is an enticing target for hostile actors, as Western societies' reliance on space-based systems is greater than ever. The space domain is interconnected to the air domain, which can easily cause cascading effects. Space-based systems can also be interfered with and damaged through ground-based systems.

Hybrid threats have been considered to target 13 different domains, namely infrastructure, economy, intelligence, information, cyber, diplomacy, political, culture, social/societal, legal, military/defence, space, and administration.[5] Hybrid threat tools affecting the space domain include, for instance, physical operations against infrastructure, creating and exploiting infrastructure dependencies, foreign direct investment, industrial espionage, cyber espionage, cyber operations, and electronic operations (e.g. jamming and spoofing). Exploiting thresholds, non-attribution, gaps and uncertainty in the law are also possible, as well as leveraging legal rules, processes, institutions and

1 D. T. Burbach, 'Early lessons from the Russia-Ukraine war as a space conflict', Atlantic Council, Essay in Content Series 'Airpower After Ukraine', 30 August 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/. [All links were last accessed on 8 December 2022, unless otherwise indicated.]

2 R. Skibba, 'Russia's War in Ukraine Reveals More Problems in Space', *Wired*, 2 August, 2022, https://www.wired.com/story/russias-war-in-ukraine-reveals-more-problems-in-space/.

3 Global space governance refers to a collection of international, regional, or national laws as well as regulatory institutions and actions, manners, and processes of governing or regulating space-related affairs or activities. The framework also includes the instruments, institutions, and mechanisms; national laws, regulations, technical standards, and procedures; codes of conduct, and confidence-building measures between space-faring actors. Definition by S. Goguichvili, A. Linenberger & A. Gillette, 'The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier?', Wilson Center, 1 October 2021, https://www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier.

4 G. Giannopoulos, H. Smith, & M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model*, Public Version, 5 February 2021, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/, pp. 9–11.

5 G. Giannopoulos et al., *The Landscape of Hybrid Threats*, p. 27.

arguments.[6] As a response to hybrid threat tools, the space domain can also be utilized to create resilience against hybrid threats and as a platform for appropriate countermeasures.

This Hybrid CoE Working Paper focuses on the following research questions:

1) How is the space domain being used in the Russo-Ukrainian war?
2) How is the space domain linked to other hybrid threat domains and what kind of tools are used?
3) Which services have been targeted and with what kind of impact?
4) Who are the main actors related to the space domain in the conflict?
5) Which space capabilities have been used to counter hybrid threats?
6) What are the implications for Hybrid CoE's Participating States?

The paper is structured as follows. First, the authors present space-based services and how they are used in the Russo-Ukrainian war. This is followed by a discussion on the use of the space domain for hybrid threat activities in the war, but also for countermeasures against hybrid threats. Major examples of space domain use are provided and links to other hybrid threat domains elaborated. The roles of selected commercial actors and services are also highlighted. Finally, conclusions and recommendations are provided.

6 G. Giannopoulos et al., *The Landscape of Hybrid Threats*, pp. 33–35.

Space-based technologies used during the Russo-Ukrainian war

Satellite technologies are used in modern society in many, often invisible ways. Satellites are a critical infrastructure enabling telecommunications, transportation, financial systems and energy networks to function reliably. Satellites provide, for example, weather data, news from remote regions, and positioning services while driving or doing sports. Typical satellite services are categorized into four main areas that include (1) Positioning, navigation and timing (PNT) services, (2) Communications, (3) Remote sensing, and (4) Science and exploration missions that typically aim to explore outer space[7] in contrast to the previous three categories, which mainly aim to support life on Earth.

Military satellite services include satellite communications and PNT as such. Monitoring capabilities are used for the following services:[8] (1) Missile warning systems, (2) Environmental and weather information, and (3) Intelligence, Surveillance, and Reconnaissance (ISR). Military space operations also include launching satellites into orbit and operating them, as well as understanding space situational awareness. The latter covers space weather services, detection and modelling of the movements of satellites and other space objects in order to understand what the opponent can see and do, and the ability to detect threats to satellites (such as space debris or missiles). Space technology is an essential supporting technology, providing the means to increase the performance of troops by improving their mobility, coordination, and accuracy of operations.[9] Space conflict is thus defined by Szymanski[10] as being "all about denying satellite support to military forces or civilian populations on Earth – not simply the elimination of satellite systems for destruction sake".

Space-based services have played an integral role in the Russo-Ukrainian war since it started. The impact of Russia's invasion of Ukraine has spread into the space domain, affecting international space collaboration and the way in which space services are used. All the abovementioned capabilities have been actively exploited and commercial companies have played an increasingly important role in supporting both military operations and civilian needs. GPS-guided weapons such as HIMARS have been used to hit targets with great precision. Satellite-based monitoring has made the battlefield possibly the most transparent in history. The exploitation of space in war does not mean that you need to have your own satellites. As has been evident in the Russo-Ukrainian war, one can exploit public and commercial satellites, and services provided by allies. Space activity has become more and more commercial, and more than 90% of all launches today are commercial satellites.[11] As of today, all military forces employ commercial satellite services as part of their operations. Ukrainian forces have used services from the

7 The European Space Agency, 'Science and exploration', https://www.esa.int/Science_Exploration.
8 U.S. Army, Space Operations, Joint Publication 3–14, 26 October 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.
9 J. Mikkola, 'Avaruussodankäynnin osa-alueet' ['Aspects of space warfare'], 11 April 2022, https://avaruusvoima.wordpress.com/2022/04/11/3-avaruussodankaynnin-osa-alueet/.
10 P. S. Szymanski, 'How to win the next space war: An assessment', *Wild Blue Yonder*, 4 April, 2022, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2981831/how-to-win-the-next-space-war-an-assessment/.
11 ESA Space Debris Office, 'ESA's annual space environment report', 22 April 2022, https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf.

likes of Starlink in their operations.[12] An important use for satellite technologies has also been to globally raise public awareness of the situation in Ukraine via sharing satellite images of Russian military convoys, constructions, aircraft deployments, and other critical events. This also highlights the importance of space in the intelligence and information domains both for the aggressor and the defender in war.

Military presence and operations in the space domain may ultimately extend to destroying space-based infrastructure in the future. Russia already demonstrated this capability by demolishing a satellite with its anti-satellite missile test in November 2021.[13] Arguably, the most important space targets will be satellites that relay data and commands directly to other satellites in remote orbits, making them choke points for critical space systems. This is particularly true for countries without extensive worldwide satellite ground control stations. However, actual space warfare will be the final frontier since nobody wants to destroy or risk their ability to use space assets. That could be the undesirable consequence since explosions in space generate a large amount of space debris that can endanger space safety and satellite services practically anywhere.

12 C. Miller, M. Scott, and B. Bender, 'UkraineX: How Elon Musk's space satellites changed the war on the ground', *Politico.eu*, 8 June 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

13 N. Drake, 'Russia just blew up a satellite – here's why that spells trouble for spaceflight', *National Geographic*, 16 November 2021, https://www.nationalgeographic.com/science/article/russia-just-blew-up-a-satellite-heres-why-that-spells-trouble-for-spaceflight.

The links between space and other hybrid threat domains

So far, the majority of the hybrid threat tools that can target the space domain exploit the linking of space assets to other domains. The space domain has previously been seen as closely related to the military/defence, economy, infrastructure, information and intelligence domains.[14] However, evidence from Ukraine reveals meaningful links to all other hybrid threat domains. Space technology and the space environment are vulnerable to hybrid threats, particularly in the cyber domain.

Satellite systems have cybersecurity vulnerabilities related to platforms and their security, the interfaces of ground-based infrastructure, and the possibility to steal and corrupt data, or even shut down the systems. Security threats related to satellite systems, focusing on satellite communications, have recently been identified[15] and there are threats that concern any type of satellite system. Jamming can affect both space and ground assets. The programmability of modern satellites enables updating the satellites in orbit to perform new operations, which opens doors to malicious applications that could be uploaded to satellites.

An example related to the Russo-Ukrainian war was a Russian cyberattack on the Viasat satellite (KA-SAT) network[16] that left modems inoperable in Ukraine and led to thousands of disruptions in organizations across Europe. The incident happened right before the invasion started, considerably impacting abilities to communicate and share situational awareness data. The ground-based intrusion entered the satellite operator's management system by exploiting a misconfiguration and then instructed a large number of residential satellite modems to drop from the network. The incident not only showed how vulnerable satellite systems are, but also revealed that integrated systems will have a higher degree of vulnerability if technologies with security weaknesses and loopholes are integrated together. Thus, when integrating terrestrial and satellite systems to function together, it is essential to create cyber-native designs, that is, to take cyber issues into account from the beginning.

The Russo-Ukrainian war has widely demonstrated that the space domain affects other hybrid threat domains both by providing tools for malicious actors and by offering resources to build resilience against the threat. There are links to all hybrid threat domains. For example, large satellite constellations can work as an alternative infrastructure to provide communication and PNT services. In the economy domain, the inability to use Russia's launching capacity has had impacts globally on commercial satellite companies, and the space industry in Ukraine has been largely disabled. Due to increased use of commercial capabilities during the conflict, Russia has claimed private space assets as legitimate targets in war, with impacts occurring in the legal domain. Table 1 summarizes the preliminary connections between space and other hybrid threat domains.

14 G. Giannopoulos et al., *The Landscape of Hybrid Threats*, pp. 28–29.
15 I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Höyhtyä, 'Security of satellite-terrestrial communications: Challenges and Potential Solutions', *IEEE Access*, 2022.
16 Viasat, 'Ka-Sat Network Cyber Attack Overview', 30 March 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/.

Table 1. Links between space and other hybrid threat domains in the Russo-Ukrainian war

Hybrid threat domain	Link/impact to hybrid threats and tools	Link to countering hybrid threats
Infrastructure	Satellite technologies are key enablers of critical infrastructure such as energy, transport and communications networks.	Large satellite constellations such as Starlink can provide an alternative communication and PNT[17] system if terrestrial infrastructure is destroyed.
Cyber	A cyberattack on satellite networks (such as Viasat[18]) can prevent communications in Ukraine and cause service disruptions in organizations across Europe. Russia is actively jamming GPS signals all around Ukraine. There have been hacking attempts targeting the Starlink system.	Space companies and nations put increased efforts into implementing space systems and ensuring that they are cyber-secure, as well as into training people to operate them in a secure way.
Economy	Space industry in Ukraine disabled.[19] Launching capacity is restricted since Russia pulled out of the collaboration.[20] Economic sanctions can be bypassed: Russia has achieved access to capabilities through allies and the black market (e.g. Russia still had access to drones via Belarus and Iran after the drone manufacturer DJI suspended business in Russia).	The private space sector finds new markets through dual-use space assets. Space priorities might be re-evaluated nationally and in international collaboration. One must be aware of the influence of other countries' investments in a targeted country's space infrastructure.
Military/ Defence	Space-based capabilities are essential for intelligence, environmental monitoring, missile warning, and command & control in the battlefield. The threat of new types of weapons, e.g. to destroy satellites, has been demonstrated by Russia.[21]	Satellites make it possible to see large-scale changes even before a crisis has emerged.[22] Historical satellite data can be used to analyze a situation before a war and to help find ways to avoid escalation. There is a need to adjust strategies and develop response options to new space weapons and diversifying space threats. New private space companies can be seen as traditional military contractors through deeper integration and partnerships. The need to protect commercial assets grows.

17 M. Kan, 'Researchers find way to use Starlink signals as alternative to GPS', *PCMag UK*, 21 October 2022, https://uk.pcmag.com/networking/143391/researchers-find-way-to-use-starlink-signals-as-alternative-to-gps.
18 Viasat, 'KA-SAT Network Cyber Attack Overview'.
19 E.g. M. Holmes, 'War Stories: Ukraine's Space Professionals Share Their Experiences', Via Satellite, 23 May 2022, https://interactive.satellitetoday.com/via/june-2022/war-stories-ukraines-space-professionals-share-their-experiences/.
20 S. Nasir 'Eight ways Russia's war in Ukraine is affecting space exploration', *The National*, 10 March 2022, https://www.thenationalnews.com/uae/2022/03/10/eight-ways-russias-war-in-ukraine-is-affecting-space-exploration/#:~:text=Eight%20ways%20Russia%E2%80%99s%20war%20in%20Ukraine%20is%20affecting,between%20Russia%E2%80%99s%20space%20chief%20and%20US%20astronaut%20.
21 M. Holmes, 'War Stories'.
22 EOS Data Analytics, 'Historical satellite images: Accessing old data', 26 August 2022, https://eos.com/blog/historical-satellite-images/.

Hybrid threat domain	Link/impact to hybrid threats and tools	Link to countering hybrid threats
Social/ Societal	Space-based capabilities can support vital functions in society during a crisis, e.g. Starlink ensured internet availability and communications in Ukraine. Citizens can provide assets to support operations, e.g. the 'dronations' campaign in Ukraine to collect hobby and commercial-use drones;[23] the crowdfunded ICEYE satellite; and crowdsourced situational awareness.	Crowd-financing is used to buy new satellites to support operations. Crowdsourcing promotes willingness to defend & psychological resilience: Grassroots action in generating military equipment supports the morale of contributors, and those on the front lines.
(Public) Administration	Commercial space capabilities and information are important for Ukrainian ministries. The Ministry of Defence supported public acquisition of an ICEYE satellite. The Ministry of the Interior uses satellite images in decision-making and for sharing information with citizens.	Satellites provide the means to connect with citizens even when the terrestrial infrastructure has been destroyed.[24]
Legal	Russia claims private space assets as legitimate targets in war.[25] Russia states the use of private satellites for military purposes to be provocative and questionable under the Outer Space Treaty. Private actors that are not happy to see their equipment used for military purposes also use legal arguments (as in the case of drone manufacturer DJI, which stated that such use is against its principles and has potential legal compliance implications).[26]	Space-based capabilities can support attribution, e.g. provide evidence on war crimes.
Intelligence	Satellites enable intelligence operations in areas that would be very challenging to work in with other means.	Satellites may reveal intelligence operations on land, detecting e.g. equipment and built areas.
Diplomacy	Russia has decided to resign from the International Space Station (ISS) collaboration. There are growing international tensions in space extending from Russia. Loss of ISS as a diplomatic tool and platform for scientific exploration in the future has a significant impact on diplomatic relations.[27]	Guidelines, actions and measures for sustainability and peaceful use of space should continue and encourage diplomatic ways out of the crisis.

23 C. Vallance, 'Ukraine sent dozens of 'dronations' to build army of drones', BBC News, 8 July 2022, https://www.bbc.com/news/technology-62048403.
24 D. Antoniuk, 'How Elon Musk's Starlink satellite internet keeps Ukraine online', 3 September 2022, *The Kyiv Independent*, https://kyivindependent.com/tech/how-elon-musks-starlink-satellite-internet-keeps-ukraine-online.
25 B. Tingley, 'Russia says private satellites could become "legitimate target" during wartime', Spece.com, 16 September 2022, https://www.space.com/russia-private-satellites-legitimate-target-wartime-united-nations.
26 C. Vallance, 'Chinese drone firm DJI pauses operations in Russia and Ukraine', BBC News, 27 April 2022, https://www.bbc.com/news/technology-61179022.
27 R. Skibba, 'Russia's War in Ukraine Reveals More Problems in Space'.

Hybrid threat domain	Link/impact to hybrid threats and tools	Link to countering hybrid threats
Political	There has been an effort by Russia to politicize the ISS, which thus far has been a purely scientific collaboration platform.[28] International collaboration between other countries and Russia is frozen and expected to remain so for an extended period of time.	The Russo-Ukrainian war has demonstrated the importance of access to satellite-based services and regional sovereignty. Small countries are learning new ways to operate if a large country attacks. For example, Taiwan has stated that it will set up a satellite-based internet if China invades.[29] Space collaboration between the EU and NATO is deepening.
Information	Russia has made provocative statements about commercial and civilian satellite assets becoming legitimate targets in wartime operations.[30] Russia's federal space agency Roscosmos has attempted to use the ISS for pro-Russian, anti-Ukrainian propaganda.[31] Influential persons in the space industry, e.g. Elon Musk, have shown support for and given guidance to Ukraine.[32]	Satellite data and high-resolution images help to challenge disinformation. Satellites are used to provide up-to-date information about events in Ukraine and areas close to it. Images are shared with the public in newspapers and online sources. Satellites enable people in Ukraine to receive international information. For example, Starlink terminals all over the country provide access to reliable sources, helping to diminish the effect of Russian propaganda.
Culture	Collaborative culture in exploring and developing space is endangered due to Russia's resignation, increasing tensions, and growing quest for strategic autonomy. Shared values can facilitate collaboration regionally or between like-minded allies.	It is possible that space collaboration in the future will be more value-based. Sustainable use of space is one example. In space security, like-minded partners are sought for collaboration. Private actors may have to position themselves culturally to collaborate. This transition is likely to make the development of a global space governance framework more difficult.

28 B. Tingley, 'Russian cosmonauts spread anti-Ukraine propaganda from space station', 6 July 2022, https://www.space.com/russia-cosmonauts-ukraine-luhansk-propaganda.
29 N. Smith, 'Taiwan plans satellite back-up amid China invasion fears', *The Telegraph*, 29 October 2022, https://www.telegraph.co.uk/world-news/2022/10/29/taiwan-plans-satellite-back-up-amid-fears-cant-rely-elon-musk/.
30 B. Tingley, 'Russia says private satellites could become "legitimate target" during wartime'.
31 B. Tingley, 'Russian cosmonauts spread anti-Ukraine propaganda from space station'.
32 Later, Musk hesitated over his support for Ukraine. See M. Holmes, 'War Stories'; B. Bender, 'Pentagon eyes locking in Starlink funding for Ukraine', *Politico.com*, 17 October 2022, https://www.politico.com/news/2022/10/17/pentagon-starlink-funding-ukraine-00062103.

Countering hybrid threats with space capabilities

Observed activities during the war

Space technologies are also actively used to counter hybrid threat operations as presented in Table 1. For example, satellites have enabled the sharing of up-to-date information and news to keep civilians and military personnel in Ukraine informed regardless of information operations over terrestrial channels. Another important factor in countering hybrid threats is collaboration among countries and leading commercial and public organizations such as NASA and ESA, and influential persons in the space industry have been showing the way, also raising awareness about the need to develop better space systems.[33] The war has deepened the collaboration between NATO and the EU via political dialogue and common messaging, providing improved capabilities for countering various types of threats such as foreign information manipulation and interference.[34] The strategic partnership is more robust than ever, supporting Ukraine to defend itself and protect its population. There are regular meetings between the EU's Political and Security Committee and the North Atlantic Council, and frequent cross-briefings between working groups. Cooperation workstrands include, for example, efforts in EU and NATO defence planning processes where requirements overlap. The war has shown that owning space capabilities is not as crucial as having access to them. This important perception may further boost international collaboration in space and the rise of the private space sector. To this end, the importance of building system redundancy and back-up systems is likely to be underlined. All in all, the group of actors that can deny access to space capabilities will become more multidimensional through privatization and diversifying space threats.

Improving the resilience of space technology

It is essential to ensure that critical space technologies will remain useful in the future. The question to be answered is how to improve the resilience of space technology and create cyber-proof systems. One way to improve resilience is to incorporate redundancy and the possibility to use several systems. In this way, failure in a single system will not prevent communication ability, for instance. A recent example showing how operations should not rely on a single satellite communication system was the announcement by Elon Musk that Starlink satellites cannot be used in Crimea.[35] Such restrictions have direct consequences for the operation of troops in that area since connections between troops and command cannot be effectively established without the use of other redundant systems.

There are multiple cyber-security threats that have not been properly taken into account when designing "old space" systems in the past. It is essential to design new systems from the

33 J. Aschbacher, Tweet, 6 October 2022, https://twitter.com/aschbacherjosef/status/1577937824971718656; M. Holmes, 'Inmarsat CEO Rajeev Suri Shares Thoughts on Viasat, IFC, Cybersecurity, and the Supply Chain', Via Satellite, 2 June 2022, https://www.satellitetoday.com/business/2022/06/02/inmarsat-ceo-rajeev-suri-shares-thoughts-on-viasat-ifc-cybersecurity-and-the-supply-chain/.

34 Council of the EU, 'EU- NATO cooperation: seventh progress report', Press release, 20 June 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/06/20/eu-nato-cooperation-seventh-progress-report/.

35 C. R. Davis, 'Elon Musk blocked Ukraine from using Starlink in Crimea over concern that Putin could use nuclear weapons, political analyst says', *Business Insider*, 11 October 2022, https://www.businessinsider.com/elon-musk-blocks-starlink-in-crimea-amid-nuclear-fears-report-2022-10?r=US&IR=T.

beginning as cyber-secure ones, specifically ensuring the security of the ground segment against ground-based attacks and vulnerabilities. The use of strong authentication and access control procedures is recommended to add system resilience. In addition, there is a need to actively monitor potential security threats in order to mitigate them with appropriate actions. This could be done using Cybersecurity Operations Centers (CSOC) that combine monitoring and decision-making technologies, human administrators, and processes to achieve accurate cyber situational awareness and to actively respond to detected threats.[36] The best CSOCs are dedicated facilities where network security analysts work continuously, focused on defending against unauthorized activity on strategic networks. They can be set up and run by nation-states or multinational corporations. In the space domain, the ESA is funding development to secure European-level operations. However, there is still a need to develop better tools for that, to train people working in the space domain – and to develop dynamic spectrum management mechanisms to protect the systems more effectively against jamming.

Means for improving the resilience and sustainability of space systems include space safety and cybersecurity, but also economic and environmental perspectives.[37] It is essential to avoid generating new space debris and to improve debris and threat detection capabilities also from space to ensure that satellite services will remain useful for coming generations. There is a need to develop better space traffic management methods, and satellites could exploit automated collision avoidance procedures to enable them to react rapidly to threats. It is also evident from the Russo-Ukrainian war that further collaboration between countries and space domain actors should be increased, and rules and measures created to ensure the peaceful use of space.

36 I. Ahmad et al., 'Security of satellite-terrestrial communications'.

37 M. Höyhtyä et al., 'Sustainable Satellite Communications in the 6G Era: A European View for Multi-Layer Systems and Space Safety', *IEEE Access*, 2022.

Main actors and forms of collaboration in the space domain during the war

Global actors

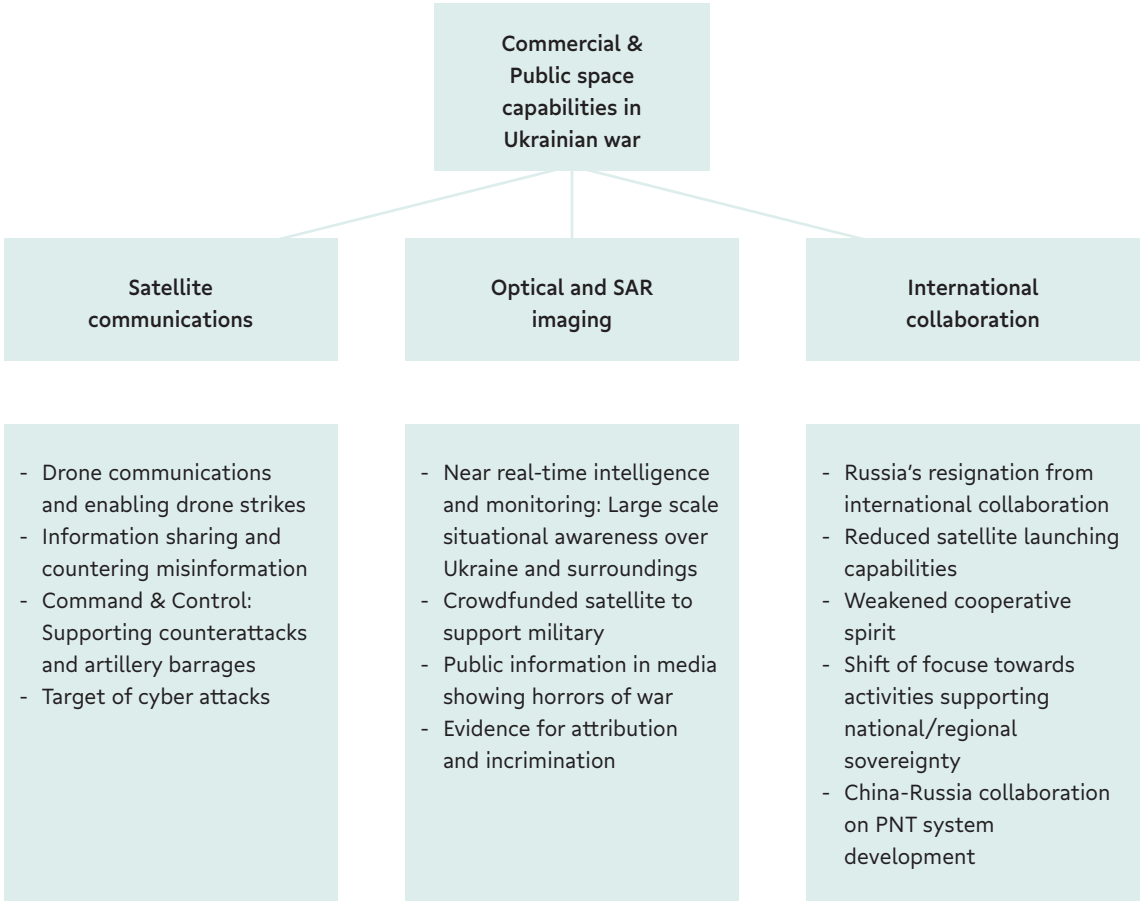
There are active global actors such as the US, the EU, China, Russia, and NATO in the space domain. The US has capabilities across ISR, GPS and connectivity, and the EU has its own flagship programmes for positioning and Earth observation (Galileo and Copernicus). The EU is also planning to build its own Secure Connectivity system called IRIS² as a new flagship and a dedicated satellite communication infrastructure.[38] It is the most significant space programme in Europe at the moment, aimed at supporting both critical users and ordinary citizens. China has the BeiDou positioning system, anti-satellite (ASAT) missile capabilities, namely the means to destroy satellites, and deep space missions including lunar rovers. Russia has long experience in launchers, human and science missions, and positioning. Finally, NATO has adopted space as its operational domain since 2019, using space to support operations and missions in such areas as communications, navigation and intelligence.[39] Through the use of satellites, NATO and its member countries can respond to crises with greater speed, effectiveness and precision.

International collaboration and launching activities

Russia has resigned from international space collaboration due to the war and this has had a major impact on international space operations and launching activities. Russia has refused to launch any further satellites for Western countries.[40] Soyuz rockets have been instrumental in constructing and supplying the International Space Station, and in keeping the station in orbit with regular boosts. Replacements are currently being sought, and fortunately SpaceX, for example, has already demonstrated its ability to launch astronauts to the ISS. However, thus far, the launches have largely affected commercial operations, and manned flights have been implemented according to plan. The effect of the war is nonetheless visible in all forms of collaboration. Recently, Russian cosmonaut and ISS commander Oleg Artemyev said that "war will end everywhere" while handing over command of the space station on 28 September to Samantha Cristoforetti, who is the first European ISS female commander.[41] The war is giving rise to new forms of collaboration as well. China and Russia announced their collaborative effort in developing positioning systems to enhance the accuracy and reliability of the BeiDou and Glonass systems to the level of GPS.[42] Both countries agreed to build satellite ground stations on each other's soil to improve the system's interoperability. However, it is already evident that the war has impacted the largely cooperative spirit of the space industry for many years to come. An overview of the situation of different space actors actively engaging in the Russo-Ukrainian war is presented in Figure 1.

38 T. Breton, 'Welcome to IRIS², Europe's new Infrastructure for Resilience, Interconnection & Security by Satellites', Statement, 17 November 2022, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_6999.
39 NATO, 'NATO's approach to space', 6 October 2022, https://www.nato.int/cps/en/natohq/topics_175419.htm.
40 M. Hilborne, 'What could be the consequences of the Ukraine war in space?', King's College London, 10 March 2022, https://www.kcl.ac.uk/what-could-be-the-consequences-of-the-ukraine-war-in-space.
41 E. Howell, 'Ukraine invasion's impacts on space exploration: Live updates', Space.com, 28 October 2022, https://www.space.com/news/live/russia-ukraine-invasion-space-impacts-updates.
42 J. Lau, 'China and Russia to boost satellite navigation systems with new ground stations', *South China Morning Post*, 30 September 2022, https://www.scmp.com/news/china/diplomacy/article/3194387/china-and-russia-boost-satellite-navigation-systems-new-ground.

Figure 1. Commercial and public activities and impacts on international collaboration during the Russo-Ukrainian war



Private companies

The role of private companies, and the services and equipment they have provided, has been essential from the beginning of the war. The role of private actors can be demonstrated by some of the key players and their impact on the Russo-Ukrainian war.

SpaceX has provided Starlink terminals and satellite capacity to support operations conducted by Ukraine. Starlink has been used to provide connections to support counterattacks or artillery barrages[43] and to enable Zoom calls from any location. The impact has been significant, especially on civilian connections, for Command and Control, and in the areas of intelligence and situational awareness. Starlink connections have been used to monitor and coordinate unmanned aerial vehicles, to send video streams from drones, and to enable drone strikes.[44] SpaceX is a significant commercial player in the satellite launch business as well. Russia used to launch many Western satellites in the past but this activity stopped abruptly due to the war. This has increased the dominance of SpaceX, which now provides launch services even for Starlink's competitors in the internet business, such as OneWeb.[45]

Maxar is operating very high resolution satellites. During the war, Maxar and other commercial operators, such as Planet Labs and Pléiades Neo, have provided high-quality images covering Russian convoys, troops, and activities at airports, which have been widely used in the press.[46] The information has played a crucial role in informing both military planning and the public view of the war.[47] The intel provided has been used from the beginning of war to obtain large-scale situational awareness data over Ukraine and its surrounding areas. Images have revealed, among other things, movements of troops and vehicles inside the country and close to it, and have confirmed damage to airplanes and infrastructure. One example of the use of the data was firstly revealing the build-up of military equipment at Zjabrovka Airport in Belarus[48] close to the Ukrainian border on 20 June, and subsequently confirming damage to the equipment caused by explosions on 10 August.[49]

ICEYE allows the Ukrainian Armed Forces to receive radar satellite imagery on critical

43 C. Miller et al., 'UkraineX'.
44 A. Freund, 'Ukraine is using Elon Musk's Starlink for drone strikes', Deutsche Welle, 27 March 2022, https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528.
45 N. Huet, 'After row with Russia over war in Ukraine, OneWeb partners with SpaceX to launch Internet satellites', Euronews, https://www.euronews.com/next/2022/03/22/after-row-with-russia-over-war-in-ukraine-oneweb-partners-with-spacex-to-launch-internet-s.
46 C. Woodun, 'Maxar: The power of satellite imagery in the Russia-Ukraine conflict', 21 April 2022, Seeking Alpha, https://seekingalpha.com/article/4502602-maxar-satellite-imagery-power-russia-ukraine-conflict.
47 M. Borowitz, 'War in Ukraine highlights the growing strategic importance of private satellite companies – especially in times of conflict', The Conversation, 15 August 2022, https://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425.
48 K. Andreikovets, 'S-400, tanks and infantry fighting vehicles. Analysts have published a satellite image of the Zyabrovka airfield, which Belarus gave to Russia', Babel, 8 July 2022, https://babel.ua/en/news/81180-s-400-tanks-and-infantry-fighting-vehicles-analysts-have-published-a-satellite-image-of-the-zyabrovka-airfield-which-belarus-gave-to-russia.
49 O. Jarmolenko, 'Satellite images from the Belarusian airfield near Zyabrovka village confirmed that there was a fire on the runway', Babel, 13 August 2022, https://babel.ua/en/news/82892-satellite-images-from-the-belarusian-airfield-near-zyabrovka-village-confirmed-that-there-was-a-fire-on-the-runway.

locations with a high revisit frequency.[50] Unlike Maxar optical data, the synthetic aperture radar (SAR) technology allows imaging through clouds and during the night, providing new opportunities to gain situational awareness data. One ICEYE satellite was bought with money raised by private Ukrainians. It was recently reported that it detected more than 60 units of enemy military equipment during its first two days of operation. Consequently, Russian troops lost armoured vehicles worth more than the cost of the entire crowdfunded satellite project.[51]

The space industry in Ukraine has long roots and was at an active stage before the war, setting up a growing private industry. However, it has been thrown into doubt due to Russia's invasion.[52] Many professionals working in startups have become soldiers. National space professionals hope that Ukraine will be able to re-evaluate space priorities and focus on security and technologies for the New Space era, with the strong emergence of private companies and the use of small satellites, and discard the remnants of the Soviet Union. A new Ukrainian space industry could then become the base for Ukraine's security and, in the long term, even support the space capability development of its allies. Ukrainian space professionals say that public support from big players such as Elon Musk has boosted morale in Ukraine, and has influenced many organizations and government leaders by pointing the way forward. If leaders in the space industry stand with Ukraine, that will work towards isolating Russia economically.

Drone technology-related actors

Drones have had a visible and significant role during the war, larger than in any major conflict to date. Thousands of different kinds of aerial platforms covering military drones, and small, off-the-shelf drones, have been used by both sides.[53] Military drones such as the Turkish Bayraktar have been used for intelligence operations to locate enemy targets, and to guide artillery fire towards them. They played a part in sinking the Moskva warship. Small, cheap drones have been used for example as kamikaze bombs, but also to spot targets and steer attacks. As a consequence of the active use of drones, counter-drone technologies such as radar systems for tracking, and directed electromagnetic pulses to disable navigation capabilities, are also increasingly being used as part of the operations.

The use of drones has linked many actors to the war. Russia has presumably obtained drones from Iran and Belarus and via black market channels after the Western sanctions, and drone manufacturer DJI suspended business activities in both Russia and Ukraine.[54] Ukraine meanwhile has deployed hobby and commercial drones donated by ordinary citizens.[55]

50 ICEYE, 'ICEYE signs contract to provide government of Ukraine with access to its SAR Satellite constellation', Press release, 18 August 2022, https://www.iceye.com/press/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation.
51 Kyiv Post, 'Satellite Purchased by Volunteers Exceeds Expectations', 29 September 2022, https://www.kyivpost.com/russias-war/satellite-purchased-by-volunteers-exceeds-expectations.html.
52 M. Holmes, 'War stories'.
53 BBC, 'How are "kamikaze" drones being used by Russia and Ukraine?', 17 October 2022, https://www.bbc.com/news/world-62225830.
54 E.g. C. Vallance, 'Ukraine sent dozens of "dronations" to build army of drones', BBC News, 8 July 2022, https://www.bbc.com/news/technology-62048403.
55 C. Vallance, 'Ukraine sent dozens of "dronations" to build army of drones'.

Actors in the information domain promoting space

Commercial satellites have had a crucial impact in the public sphere through satellite imagery demonstrating the horrors and consequences of the war to the media and people, duly shaping public opinion, and eventually even Ukraine's foreign policy.[56] Information has served to boost morale: Ukraine has been able to use space in gaining data and thus factual evidence for countering Russian propaganda. It has revealed Russia's weak points and facilitated Ukrainian success in its military activities through precise data whenever possible. Finally, satellite data has supported analysis of the war both for media and military experts in the defence sector, as well as academia.

The role of influential individuals has been visible in the information domain linked to space. SpaceX founder Elon Musk has issued strong, even provocative statements to gain support for Ukraine, but has also ambivalently highlighted the possible discontinuation of the satellite services due to funding problems.[57] At the other end of the spectrum are then Roscosmos chief Dmitry Rogozin's attempts at pro-Russian and anti-Ukrainian propaganda, and threats to pull out of ISS collaboration. Legal and ethical aspects have been a part of Russia's information activities (declaring the commercial satellites targets of war, and blaming Ukraine and the West for breaking the Outer Space Treaty).

The impact of information campaigns is difficult to evaluate, but despite Russia's intentions and attempts to the contrary, the utilization of the information domain has eventually smoothed the path for Ukraine as it has made the war visible and kept it in the public eye. Ukraine has gained amazingly solid support from Western countries. For instance, the EU and the Pentagon have considered funding the Starlink satellite network for Ukraine.

56 J. Siegel, 'Commercial satellites are on the front lines of war today. Here's what this means for the future of warfare', Essay in Content Series 'Airpower After Ukraine', 30 August 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/.

57 B. Bender, 'Pentagon eyes locking in Starlink funding for Ukraine'.

Discussion and conclusions

Space has had an important role since the beginning of the Russo-Ukrainian war, and military forces have effectively used commercial capabilities from European and US service providers to enable their operations. The war has shown that the space domain was crucial before the escalation of war, namely in the sub-threshold[58] phase, as well as during the war. It will also be necessary in the aftermath, for instance when assessing the damage to and security of areas and providing evidence for legal attribution. The space domain affects other hybrid threat domains both by providing tools for malicious actors and by offering resources to build resilience against threats. Space technology and the space environment are vulnerable to hybrid threats, especially in the cyber domain, and cyber attacks against satellite communications systems have had significant effects not only in Ukraine but also in other areas.

The space domain in war has affected both military operations and the security of civilian society in Ukraine. On the other hand, civilian actors have been empowered to support the war with the help of space-based capabilities. The information domain has exploited space-based capabilities to illustrate and narrate the war. The war has had a large impact in many countries in removing the stigma of military technologies. While before the war there was a large number of organizations that did not want to associate themselves with the military field at all, many commercial companies are now proudly presenting the dual-use capabilities of their products. This could lead to increased support for military capability development in the EU and NATO countries, as the capabilities are perceived to bolster the resilience of society more widely. The interest in including dual-use technologies in industrial collaboration in strategic defence capability development projects may increase. This will also raise the issue of governments' willingness and capability to protect commercial assets.

The main actors in the conflict from the space domain point of view have included global actors such as the US, Russia, NATO and the EU, but also the unprecedentedly increasing role of private companies and their space assets. SpaceX in particular has increased its global role as a provider of both communications technology and launching services. Crowdsourcing situational awareness with the help of Starlink, and crowdfunding as a tool for financing space capabilities, have demonstrated the growing role of individuals as security actors in modern societies. If used efficiently, this development will promote comprehensive security and build resilience in the future. This type of empowerment may, however, work both ways, which means that the role of individuals in malicious activities deploying space capabilities may grow in the future, duly altering and increasing the hybrid threat potential. However, the legal responsibilities of governments and authorities will not disappear despite the blurring roles of security actors. Individuals can contribute to security but they cannot be considered accountable for ensuring it, as only authorities have jurisdiction defined by law.

The war will have a long-term impact on the development of the space domain through changes in collaboration forms and settings, space capability re-prioritization,[59]

58 Going beyond the threshold triggers a response towards the hostile actor. The sub-threshold phase refers to a phase during which hostile hybrid threat activities occur, but the threshold for a conventional response has not been reached.

and increased as well as more versatile use of commercial technologies and services. Simultaneously, the war has increased regional efforts towards strategic autonomy, such as Europe's goal to implement its own satellite communication constellation.

Preliminary implications based on this study can be summarized in four key takeaways:

1. The power of crowdsourced situational awareness has been demonstrated in the war. However, it is partly unclear how one can verify the crowdsourcing data and prevent the inclusion of intentional malicious data in decision-making. Space technology could have a relevant use here, for example by verifying the reported events with satellite imaging. The role of citizens in supporting the operations has grown, raising legal questions about the responsibilities and role of authorities.
2. The Russo-Ukrainian war has paved the way for satellite-based technologies to turn into easily accessible everyday tools for both military and civilian populations. This can not only promote resilience against hybrid threats in the military domain, but also psychologically. The ability to contribute in a crisis and war situation, and to do something concrete and tangible, will promote and sustain individuals' psychological resilience and willingness to defend. Resilience can also be supported via the information domain: in a crisis, people call for up-to-date information on the situation. Data retrieved via satellites will help to fulfil this need. It can also benefit information campaigns countering hybrid threats, as well as people's resilience against influencing activities in the information domain.
3. The use of commercial space assets in military operations is blurring the line between military and civilian actors in the war. People in Ukraine have collected money to buy a satellite to support operations, which has already been used successfully in military operations. Commercial actors do not necessarily even know that their technology is dual-use. Thus, the decision to be involved in the war is unintentionally outsourced to someone using the technology of commercial actors. This can be ethically problematic, as some actors would like to stay out of the war or choose their side and deny hostile actors access to their assets. Assessing the threat in the space domain – namely the capabilities and actors posing the threat, as well as assessing the potential impact – becomes increasingly difficult.
4. Developments in satellite technologies and their use also foster new combinations of capabilities that can be used for military purposes. Drones have had a significant impact on Ukraine's operations and will have a salient role in future conflicts elsewhere. Hence, states should develop their capabilities in drone and counter-drone technologies. When drones are equipped with satellite connectivity, they can be used effectively over very large areas, a development that is also supported by the European Space Agency. It is evident that air forces will need to pre-

59 National development of space capabilities depends on global space priorities. For instance, after the war, Ukraine could pay more attention to security, small launch vehicles, satellite technologies, and communication. M. Holmes, 'War Stories'.

pare themselves for drone operations more frequently. The role of drones is also likely to grow in the sub-threshold phase. In addition to the military, drones may pose an increasingly severe threat to other security authorities and vital functions of society, such as critical infrastructure.

Authors

Marko Höyhtyä works as a Research Professor at the VTT Technical Centre of Finland, focusing on satellite communications and situational awareness technologies. In addition, he holds the title of docent (associate professor) at the National Defence University (Finland). He has contributed to this paper as an independent researcher, and hence the perspectives and analysis presented here should not be considered the official views of VTT.

Dr Sari Uusipaavalniemi is a Senior Analyst in the Community of Interest Vulnerabilities & Resilience at Hybrid CoE, on secondment from the Finnish Defence Research Agency. She has solid experience in the Finnish Defence Forces (FDF) in different research and expert positions. Her interest areas include strategic foresight, resilience, comprehensive security, and space security.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats