CSS Analyses in Security Policy

No. 333, December 2023

The New Frontier of Space Militarization

The exploitation of space today is increasingly driven by the innovations of private actors. Confronted with Russia's military aggression, Ukraine showed how nations with little or no space capabilities can leverage commercial space infrastructure for combat. The massive reliance on commercial actors to provide vital support for Ukraine's military operations suggests a new round of the militarization of space, one that private actors increasingly dominate.

By Sarah Wiedemar

A Ukrainian soldier disconnects their Starlink during a ceasefire over the Orthodox Christmas period in Kreminna, Ukraine in January 2023. *Clodagh Kilcoyne / Reuters*

The civilian use of space has always gone hand in hand with its military use. During the Cold War, the Soviet Union's launch of Sputnik 1 in 1957 and the US's deployment of Explorer 1 in 1958 kicked off the space race between the two superpowers. As early as 1962, the US began to commercialize space with the launch of Telstar 1 – the first commercial communications satellite. In the same year, Congress passed the Communication Satellite Act with the aim of affirming the rights of private companies to own and operate commercial satellites.

The technology used in the space industry is inherently dual use in character. For instance, ballistic missiles can be used to carry nuclear warheads; however, the same technology can also be used for civilian purposes to launch satellites into space. Likewise, satellites orbiting the Earth can fulfill civilian functions such as supplying global positioning and navigation information, capturing satellite imagery to detect wildfires, and providing access to the internet in remote locations. However, the same technologies behind these functions – and sometimes even the same satellites – are increasingly used for military purposes. For example, they can provide early warning of missile attacks, immediate damage assessments, and the identification of enemy targets via satellite imagery. They can also enable real-time data exchange on the battlefield to synchronize military operations involving multiple units.

The first demonstration of the successful integration of space-based assets into a military operation occurred during the Gulf War in 1991 – also widely referred to as "the first space war." The US Armed Forces heavily relied on both civilian and military satellites for navigation, communication, intelligence collection, and missile guidance. In particular, the reliance on the US Global Positioning System (GPS) highlighted inherent issues with the dual-use character of most technologies in the space domain.

The US Department of Defense envisioned GPS in 1973 as an experimental satellite navigation program, one that civilians would eventually also be able to access. Since GPS was originally designed as a military support system, the US intentionally reduced its accuracy for civilian use through selective availability. This proved problematic during Operation Desert Storm when the US Army required more GPS signal receivers than the military could provide. They purchased and used commercial GPS receivers that were not designed for a battlefield environment, and thus had a lower degree of accuracy. As the selective availability feature of commercial devices hindered the use of GPS by the US military during the Gulf War, it was switched off for this period. The successful use of GPS in the Persian Gulf conflict gave the commercial GPS market a major impetus in the following years. However, it also exposed the military nature of the GPS service, highlighting potential implications for the users who depended on it around the globe. In 1991, the European Commission hinted that it planned to develop an EU satellite navigation system to reduce Europe's dependence on GPS. Two decades later, the EU and the European Space Agency (ESA) jointly launched the Galileo satellite navigation system, which provides a global positioning service under civilian control.

Space-based assets have been essential to Ukraine's warfighting capabilities.

In the early 2000s, the commercial space industry gained new momentum. Gradual deregulation and an influx of venture capital kicked off the growth of private commercial space ventures. Market pressures forced companies to heavily invest in innovation solutions across engineering, procurement, and business development to lower customer costs and increase competitiveness. As a result, the cost of accessing space was significantly reduced due to lower-cost launch systems, reusable rockets, and standardized nanosatellite designs (so called CubeSats). This also led to greater diversification in the space sector, with new companies entering a domain traditionally dominated by established defense industry players (see CSS Analysis no 256).

The growth of the commercial satellite sector has rapidly increased the militarization of commercial space assets – a trend best exemplified by the ongoing war in Ukraine. General John Raymond, head of the US Space Force, described the war as the first where commercial space capabilities have played a significant role. From satellite imagery provided by a multitude of commercial providers to Elon Musk's Starlink constellation facilitating high-speed Internet, space-based assets have been essential to Ukraine's warfighting capabilities. The extensive use of commercial space assets to support Ukrainian military operations suggests that the strategic value of space is here to stay. This also indicates that private companies will have a major stake in this new round of space militarization.

Commercial Actors in Ukraine

With no satellites of its own, Ukraine is highly dependent on Western commercial space companies to conduct its military operations on the ground. In its ongoing conflict with Russia, Ukraine exemplifies the substantial utilization of commercial satellite technologies for military operations. However, Kyiv's reliance on non-Ukrainian satellite providers for military purposes has also created new risks and vulnerabilities for the commercial providers themselves. Though these satellite providers may not have intended this themselves, they have been militarized, blurring the distinction between the military and civilian application of their technologies. When, as a result of such a situation, a commercial satellite provider is targeted by a belligerent party, its regional userbase or global operations can be impacted. Such cascading effects outside a conflict zone could, in turn, result in new geopolitical or escalation dynamics. This also shows how these private institutions can become part of an international armed conflict and caught up in the tensions between different stakeholders.

The next section includes a selection of space technologies, related systems, and companies that illustrates how Ukraine harnesses commercial space assets. It also points out the implications of the use of such technologies in a military context.

GIS Arta

Following the Russian invasion of the Donbas in 2014, Ukrainian volunteers developed the Geographic Information System for Artillery (GIS Arta). GIS Arta is a software solution that functions like the Uber app, which connects riders with drivers in real time. It links different locations, sensors, and artillery units to allocate fire missions to the most suitable units. It also displays enemy positions on a digital map and uses algorithms to optimize variables such as the target type, position, and distance. This automated process significantly reduces the time between target acquisition and firing, and thus enhances operational efficiency.

GIS Arta has been deployed in a variety of setups and can be used on mobile phones, tablets, and laptops. It is usually installed on a rugged device (i.e., one made for operations in harsh environments) and uses either a radio for short-range data transmissions or a satellite uplink for long-range data exchange. Prior to February 2022, GIS Arta exclusively relied on the KA-SAT satellite network, operated by the company Viasat. This was due to the absence of any other reliable satellite communications provider being willing or able to provide low-cost coverage in Ukraine. GIS Arta's reliance on Viasat was not unusual at the time, as Ukraine's military, police, and intelligence services purchased Viasat modems to connect to KA-SAT as well.

On 23 February 2022, just hours prior to the Russian invasion, Viasat fell victim to a malicious cyber operation designed to cripple Ukraine's command and control systems. The operation consisted of two separate attacks carried out at the same time. One was a wiper malware, deployed to take out between 40,000 and 45,000 KA-SAT modems. The second involved the attackers flooding the Viasat network with requests to overload the system. The attacks resulted in collateral damage extending beyond Ukraine, disrupting broadband satellite Internet access for several hundred thousand customers across Europe. Critical infrastructure in Germany was also affected, leading to the loss of the remote monitoring and control of 5,800 wind turbines. The extent of the impact on Ukrainian military's communication setup remains unclear. The US, the UK, and the EU attributed this offensive cyber operation to the Russian military intelligence agency, also known as the GRU. Since the attack against Viasat, the Russian military has steadily increased its efforts to disrupt satellite communications in Ukraine. According to TASS in October 2023, Vladimir Yermakov, director of the Russian Foreign Ministry's department for non-proliferation and arms control, warned that quasi-civilian infrastructure in space that the US and its allies use in the conflict in Ukraine may become legitimate targets for retaliation.

Starlink

The outage of Viasat in the early hours of the Russian invasion prompted Ukrainian officials to look for alternative satellite communications providers. On 26 February

2022, Ukrainian Minister of Digital Transformation Mykhailo Fedorov directly addressed the founder and CEO of SpaceX, Elon Musk, via Twitter with an urgent request for the provision of Starlink terminals. Starlink was the first low Earth orbit (LEO) satellite constellation to provide broadband Internet. With 4,500 satellites in low orbit, it is also currently the largest satellite constellation. Within a few days of Fedorov's post, SpaceX delivered thousands of backpack-sized terminals to Ukraine. These terminals, which are easy to set up and use, provide civilians with high-speed satellite Internet, which proved to be invaluable for reestablishing connectivity in areas where digital infrastructure had been destroyed. Beyond its civilian use, Starlink is utilized by the Ukrainian military. Starlink enables access to real-time intelligence and allows Ukrainian commanders to communicate with frontline units. Images and GPS coordinates of Russian troop positions are also shared via these channels with artillery units to coordinate missions. In addition to communication, Starlink enables high definition drone feeds, used for both reconnaissance and attacks on enemy positions when equipped with small bombs or anti-tank grenades.

Ukraine capitalizes on satellite imagery from various leading Earth observation companies.

Starlink has a significant impact on Ukraine's military operations, prompting Russia to ramp up its efforts to disrupt the satellite constellation and its services. While SpaceX has acknowledged numerous attempts to jam its satellite signals and even hack its networks, Starlink has remained resilient and overcome such efforts, at least as of the time of writing. However, the use of Starlink by the Ukrainian military presents challenges for the company and its userbase beyond Ukraine. According to Elon Musk's biographer Walter Isaacson, the Russian ambassador to the US had also warned Elon Musk in 2022 that any attack on Crimea could lead to a nuclear conflict. In February 2023, SpaceX clarified that Starlink was never intended to be weaponized and that the company had acted to prevent the Ukrainian military from using the service to control drones. As a result, the Ukrainian military experienced Internet outages on the frontlines and in Russian-occupied territories. Musk emphasized that activating Starlink for sensitive operations would explicitly involve SpaceX in a major act of war and conflict escalation. Concerns also arose about the financial implications of providing Starlink services to Ukraine, costing an estimated 20 million USD per month. SpaceX emphasized its inability to sustain Ukraine's free use of its services indefinitely, and thus pressured the US Department of Defense to assume funding responsibilities.

Ukraine's dependence on a US-headquartered company during an international armed conflict is also a new situation for policymakers in Washington. In June 2023, the US Department of Defense signed a contract with SpaceX to cover the cost of Starlink satellite services for Ukraine. The deal also included the purchase of 400-500 Starlink terminals, which allowed the Pentagon to gain control over the Starlink signal set up in Ukraine to prevent service outages for specific missions and regions. The Ukrainian government has also been seeking to reduce its dependence on Starlink by talking to other satellite communications providers, such as Satcube from Sweden. However, Starlink's dominant position in providing satellite Internet technology remains in place for the time being, and it is often the only service that offers access to fast connectivity in regions affected by conflict or disasters. In addition, during the 2022 anti-government protests in Iran, Starlink allowed activists to circumvent government online censorship measures. In October 2023, Elon Musk also offered Starlink services to humanitarian organizations operating in the Gaza Strip.

Satellite imagery

In addition to satellite communications, Ukraine also capitalizes on satellite imagery from various leading Earth observation companies. In the months leading up to the 2022 invasion, US intelligence agencies more than doubled their acquisition of commercial electro-optical images over Ukrainian territory and made these available to Ukraine and others. For example, this included satellite images from the US-headquartered company Maxar Technologies that documented Russia's military buildup along the Ukrainian border. These were widely covered in the media.

Like he did with Starlink, Mikhailo Federov contacted leading commercial satellite companies on Twitter, urging them to supply Ukraine with high-resolution satellite imagery. In particular, he asked for imagery from satellites equipped with synthetic aperture radar (SAR). Unlike optical technology, SAR enables all-weather observation, day and night.

Among others, Canadian satellite company MDA heeded Federov's call. In March 2022, the company received special authorization from the Canadian government to use its Radarsat-2 satellite to collect SAR imagery to assist Kyiv. MDA also participated in an international effort with other commercial providers to merge and analyze their images to supply the Ukrainian government with comprehensive satellite imagery intelligence reports.

Another important contributor for Ukraine is the Finnish company ICEYE, which operates the largest SAR satellite constellation. The Ukrainian charity foundation Serhiy Prytula raised enough money to sign an exclusive contract with ICEYE, granting access to the full capacity of one of the company's SAR satellites for the Ukrainian military. In addition, the Ukrainian government regularly receives radar satellite images of critical locations from ICEYE.

Ukraine has expanded on how it taps into this pool of commercially available data from leading companies. These companies were committed to assisting Ukraine in its defense against Russian aggression. However, this support may obviously depend on conflict dynamics and context. The political views of companies can change, and financial considerations can also impact their decisions.

Palantir

Since its foundation in 2003, Palantir has succeeded in establishing a dominant mar-

Further Reading

Clémence Poirier, **"ESPI Short Report 1 – The War in Ukraine from a Space Cybersecurity Perspective,"** *European Space Policy Institute (ESPI)*, 2022.

Adam Satariano / Scott Reinhard / Cade Metz / Sheera Frenkel / Malika Khurana, **"Elon Musk's Unmatched Power in the Stars,"** *The New York Times*, 28.07.2023.

Laetitia Cesari, **"Commercial Space Operators on the Digital Battlefield,"** *Centre for International Governance Innovation*, 29.01.2023.

OECD, **"How the War in Ukraine is Affecting Space Activities. New Challenges and Opportunities,"** *OECD Policy Responses on the Impacts of the War in Ukraine*, 15.11.2022.

ket position in algorithmic intelligence software with a focus on warfare. The US company's leadership has repeatedly been vocal about its commitment to Western values, pursuing an approach aimed at defending liberal democracies, US allies, and partners, including Ukraine.

In June 2022, Palantir CEO Alex Karp was the first head of a large Western corporation to personally visit Kyiv and meet Ukrainian President Volodymyr Zelensky after the invasion. Palantir subsequently made its artificial intelligence software MetaConstellation available to Ukraine, and the country integrated the software into its military operations. The software imports commercial satellite and other imagery from different vendors, including SAR, thermal, and other satellite imagery, and provides a comprehensive assessment of ground locations of interest at specific times. MetaConstellation detects military targets and predicts their future movements by using Palantir's Edge AI technology. By doing so, the software enables rapid target acquisition within 30 seconds, making this tool highly effective for combat situations. Like GIS Arta, MetaConstellation relies on the broadband connection provided by Starlink. Palantir is responsible for most of the detection and identification of targets in Ukraine. The lack of alternative software for these tasks highlights Ukraine's dependence on the company.

The providers of satellite Internet and imagery may be in a position to decide which belligerents to support and what sort of support they provide, if any.

Outlook

There is currently a wave of ambitious projects for satellite mega-constellations in LEO orbit driven by both the private sector and government initiatives. In addition to Starlink, other satellite Internet players such as Eutelsat Group's OneWeb and Amazon's Project Kuiper plan to deploy tens of thousands of satellites. Similar efforts are being undertaken by the Chinese government, whose planned Guo Wang mega-constellation might consist of up to 13,000 satellites in LEO orbit. The European Union also aims to build a sovereign European satellite communications constellation, called Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS^2). The aim of this constellation is to present a European solution to the current dominance of the satellite communications market by US companies. As such, it will likely strengthen Europe's strategic autonomy in space for European military and civilian users.

It is also important to note that the massive deployment of satellites in LEO orbit creates significant challenges for satellite traffic management in space. Because the LEO orbit is increasingly congested, the likelihood of accidents and satellite collisions is rising. Similarly, the creation of these massive constellations will highly likely have geopolitical implications. For instance, in situations of international armed conflict, the providers of satellite Internet and imagery may be in a position to decide which belligerents to support and what sort of support they provide, if any. This would potentially leave private companies in a position to conduct foreign policy decisions that will have a direct impact on the battlefield, without their host governments having a say.

The Taiwanese government has learned from the experience of Ukraine. For example, it has reached out to the UK satellite communications provider Eutelsat OneWeb, currently Starlink's biggest competitor in LEO satellite Internet services. In June 2023, the Taiwanese Ministry of Digital Affairs stated that OneWeb is expected to provide the whole of Taiwan with satellite internet by the end of 2023. This forms a part of efforts by Taipei in recent months to find alternatives to its current information infrastructure. Should China attempt to cut off Taiwan by destroying the undersea cables that currently connect the island to the Internet, satellite communications would be critical to maintaining connectivity during a potential Chinese invasion.

Looking to the future, the militarization of space will intensify. Commercial space entities will also play an ever-increasing role in international armed conflicts. The decisions that these companies will make based on their own strategic interests, foreign policy, and legal and ethical considerations will influence the outcomes of conflicts on Earth and the future peaceful use of space.

For more on cyber security, see CSS core theme page.

Sarah Wiedemar is a Researcher in the Cyberdefence Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language editing: Mike Woods
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

Assessing Hybrid War: Separating Fact from Fiction No. 332
The Role of Mediation Support Structures No. 331
UN Peacekeeping No. 330
German Military Planning: Aims and Trade-Offs No. 329
Managing Disaster Costs No. 328
Central Asia in an Era of Great-Power Rivalry No. 327

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000644277