CHAPTER 13

The Space Domain and the Russia-Ukraine War

Lonneke Peperkamp & Patrick Bolder

Abstract

This chapter focuses on space as an operational military domain. How is space technology used in the Russia-Ukraine war? After a brief historical overview of the military use of space, four specific capabilities are analysed: space force enhancement through satellite communication (SATCOM); intelligence, surveillance and reconnaissance (ISR); position, navigation, and timing (PNT); and space control through offensive and defensive counter-space capabilities. This analysis underlines that space technology is increasingly important for military operations. In the Russia-Ukraine war, it has enabled unprecedented transparency, supported logistics, increased precision in targeting, and has played a key role in exposing enemy locations, potential war crimes, humanitarian crises, and environmental damage. Interestingly, many capabilities are provided by commercial actors, such as Maxar and SpaceX. The way in which space technology is used, however, also tends to blur the military-civilian lines. That raises challenges related to an increased civilian risk and growing power of commercial players.

Keywords: Space technology, Warfare, Space force enhancement, Counter-space

1. Introduction

The Gulf War of 1991 is often called the first 'space war,' as it was the first conflict in which space technology played a critical role. Since then, the use of space technology in military operations has become increasingly important and widespread. The importance of space technology also means that counter space capabilities, i.e. means and methods to disrupt, degrade or destroy space systems, are proliferating, as these help to protect one's own capabilities and can be used to counter the strategic advantage of adversaries. Given the increasing militarisation and weaponisation of space, political analysts and academics have raised alarms on the growing likelihood of 'space warfare'; space turning into a battlefield.

The Ukraine conflict allows us to see where we stand today. What is the role of the space domain in the Russia-Ukraine war? What lessons can be drawn from that use of space technology in warfare? In this chapter, we will briefly show how the

militarisation and weaponisation of space has evolved and distinguish various (counter) space capabilities. Against that backdrop, we will analyse how space technology is used in this armed conflict. It will become clear that, although space warfare in the sense of exploding satellites does not take place, space technology continues to be a crucial enabler for military operations, but far more prominent and extensive than three decades ago. Based on that overview, we will draw attention to challenges that arise from this use of space, and which relate to civilian risk and the power of commercial players. By the end of this chapter, we aim to provide a more comprehensive understanding of the role of space technology in modern warfare and how it is shaping the conduct of military operations in the Ukraine conflict and beyond.

2. Militarisation and weaponisation of space

Since the dawn of human space exploration, the militarisation of space has been an undeniable reality. The launch of Sputnik 1 in 1957 marked the onset of the first Space Age. Two contrasting perspectives emerged simultaneously: one in which space is a sanctuary for the betterment of humanity, to be used for peaceful purposes only, and another in which space is a crucial security environment necessitating control and dominance. During the first Space Age, space capabilities primarily served military intelligence and reconnaissance purposes, the support of ground-based weapons, and for ballistic missiles and missile defense systems. The two superpowers were also the sole space powers, and Russia and the USA conducted various experiments to weaponise space.[1]

The American invasion of Iraq, known as Operation Desert Storm, and the subsequent expulsion of Saddam Hussein's forces from Kuwait would not have been possible without satellite observation, communication, and navigation.[2] The movement, positioning, and communication in the desert as well as the preparation for ground manoeuvres relied on secure and stable satellite communication. Satellite information played a significant role in identifying targets during the 42-day-long pre-ground war air offensive. The precise positioning and synchronisation of military units depended on the Position, Navigation, and Timing (PNT) signals provided by the military Global Positioning System (GPS) through satellites orbiting approximately 20,000 km above the earth's surface. This marked the first time in history that armed forces relied heavily on space technology to support ground-based warfare.[3]

[1] Caldicott and Eisendrath, *War in Heaven: The Arms Race in Outer Space*, 11.

[2] Anson and Cummings, "The first space war: The contribution of satellites to the gulf war," 45-53.

[3] Steer and Stephens, *War and Peace in Outer Space*, 25.

Since then, we have entered a period often referred to as the second Space Age. Space technology has become an integral part of everyday life on Earth, as it is a key technology that enables e.g. the Internet, telephone communication, weather forecasts, traffic and aviation, and the banking system. Besides the two former superpowers, numerous other states and commercial actors have entered the arena, increasing the number of satellites exponentially.[4] Because space infrastructure is a critical enabler for both critical civilian infrastructure and military operations on Earth, an increasing number of states aim to protect free access to space capabilities, including by military means. The perspective in which space is a sanctuary for humanity appears to have taken a backseat. Space is now becoming increasingly militarised, with many states fully integrating the space domain into their doctrines and military strategies. NATO has formulated an overarching space policy, officially recognising space as an operational military domain.[5] Multiple states have established dedicated branches within armed forces and are strengthening their own capabilities.

That goes hand in hand with the proliferation of means and methods to 'deceive, disrupt, deny, degrade, or destroy space systems.'[6] Such counter-space capabilities can be used defensively to counter threats and offensively to counter the strategic advantage of adversaries. A notable example is the Russian DA-ASAT Nudol system.[7] Russia demonstrated its kinetic ASAT capability by testing this missile a few months before the invasion of Ukraine.[8] The increasing operational significance of counter-space capabilities is illustrated by the recent activation of the 75th Intelligence, Surveillance and Reconnaissance Squadron in the US: the first unit within the Space Force tasked with not only target analysis (providing intelligence on enemy (counter) space capabilities) but also target engagement; the actual targeting of enemy satellites, ground stations and/or communication links between them.[9]

[4] Navigation systems, air traffic control, train operations, traffic management systems adapting to congestion, internet and cellphone services, banking and stock exchange operations, energy providers and stations, weather forecasting, climate research, and pollution detection all heavily rely on the utilisation of space and its satellite infrastructure.

[5] The five military domains according to NATO doctrine are: Sea, Land, Air, Cyberspace (also called Information domain) and Space.

[6] Weeden and Samson, *SWF: Global Counterspace Capabilities: An Open Source Assessment.*

[7] Weeden and Samson, *SWF: Global Counterspace Capabilities. An Open Source Assessment*; Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

[8] Whilst the test was arguably in violation of international law (Zwanenburg, Peperkamp, Siemensma, 2021), the critique did not invoke the Outer Space Treaty or any other international regulations. Since then, however, Kamala Harris declared that the US would not conduct destructive ASAT tests (anymore) and since then an increasing number of states signed the same declaration, including the Netherlands.

[9] Friend, "Space Force's first targeting squadron brought to life"; Tingley, "US Space Force creates 1st unit dedicated to targeting adversary satellites."

As is clear, armed forces use space technology in various ways. These contemporary capabilities can be divided into various mission areas: 1) space situational awareness (SSA) that provides information on space infrastructure, potential threats, and space weather; 2) space force enhancement to increase the effectiveness of military operations through satellite communication (SATCOM), detection and shared early warning (SEW), intelligence, surveillance and reconnaissance (ISR), observation of weather conditions (METOC), and position, navigation and timing (PNT); 3) space support which enables the launch, maintenance and use of space systems; 4) space control through defensive or offensive counter-space capabilities; and 5) space force application where space based weapons could be used to engage targets on earth.[10] These developments and capabilities indicate that space technology does no longer serve solely as a critical enabler of warfare on earth, but that space is emerging as a warfighting domain. Indeed, many experts recently came to see space as a potential battleground, as states prepared for warfare from, through, or even in space.[11] Moreover, it seems that we have now entered the third Space Age, which is characterised by commercial-military cooperation.[12] As will be clear in the analysis of the Russia-Ukraine war, this comes with its own peculiarities, advantages and vulnerabilities.

Against the backdrop of these advancements in the realm of space, we now turn our attention to the ongoing armed conflict, which started with the invasion of Ukraine by Russia on February 24th, 2022. How is space technology utilised? And do these capabilities provide strategic advantages? In the following sections, we will use the distinctions highlighted here to delve into three types of space force enhancement that hold significant relevance – ISR, SATCOM and PNT – and space control through counter-space capabilities.

3. Intelligence, surveillance, and reconnaissance (ISR)

In the days before the Russian invasion of Ukraine, the whole world witnessed the buildup of troops, a new field hospital, and a pontoon bridge close to the Ukraine border – despite Russian withdrawal claims. Space-enabled ISR made this possible; high-resolution images were provided by US-based company Maxar, known for its involvement in building electro-optical satellites (remote sensing) since 1993. Commercial satellite imagery also showed the tactical errors and strategic blunders resulting from Russia's initial incorrect assessment of Ukrainian resistance.

[10] Dutch Air and Space Doctrine and Defense Space Agenda.

[11] Steer and Stephens, *War and Peace in Outer Space*, 25.

[12] Shaw, "Welcome to the Third Space Age."

It revealed a line of stationary military vehicles northeast of Kyiv on their way to occupy the Ukrainian capital. It stretched to a length of over 60 km.

Other commercial actors played a similar role by providing electro-optical imagery to the media.[13] US company Planet, for example, enabled assessments of the environmental damage, including in areas that were not freely accessible. It showed the damaged oil depot in Lviv, the Irpin River Dam and forests in the Kharkiv region.[14] Also, satellite imagery was used after the destruction of the Nova Kakhova dam and hydropower plant to track flooded houses and their inhabitants and to assess environmental damage and changes to the Dnipro waterways. Moreover, such imagery can contribute significantly to war crimes investigations and truth-finding. It showed for example how the bodies found in Irpin and Bucha along the roadside were there since the Russian occupation, and not after, as Russian disinformation tried to make us believe. Extensive reporting in the New York Times on April 4th, 2022 highlighted this.[15]

Aside from electro-optical satellites, valuable information is provided by radar satellites. One of those, a used Finnish Iceye satellite, was acquired last year by the Ukrainian government through a crowdfunding campaign. The radar of this 'people's satellite'[16] is able to penetrate clouds and can contribute to situational awareness even during the night or when it is cloudy. These images helped to identify Russian military equipment, weapons and combatants.[17] Additionally, information was provided by commercial actors: 'Radio-frequency data providers like HawkEye 360 and Spire Global used satellites to track Russian GPS jammers.'[18] Nearly half of the available satellite imagery came from such commercial actors.[19] Aside from strategic advantages of ISR for Ukraine, the availability of information has had significant wider benefits for the general public. Because of the public disclosure of information, these companies significantly contributed to 'promoting global transparency and combatting the spread of disinformation' – an essential factor shaping the war's narrative.[20]

[13] Erwin and Werner, "Dark clouds, silver linings: Five ways war in Ukraine is transforming the space domain."

[14] Ovsyaniy, "Satellite images reveal how Russia's Invasion has devastated the environment in Ukraine."

[15] Browne, Botti, and Willis, "Satellite images show bodies lay in Bucha for weeks, despite Russian claims."

[16] Watkins, "Finnish company to provide Ukrainian army with satellite imaging."

[17] Ukrinform, "'People's satellite' helps spot thousands of units of Russian equipment."

[18] Erwin and Werner, "Dark clouds, silver linings: Five ways war in Ukraine is transforming the space domain."

[19] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

[20] Erwin and Werner, "Dark clouds, silver linings: Five ways war in Ukraine is transforming the space domain."

But collaboration with commercial space actors for ISR purposes is not limited to Ukraine or its allies alone. Chinese based satellite manufacturer Changsha Tianyi Space Science and Technology Research Institute Co. LTD (Spacety China) appears to have enabled Wagner's combat operations by delivering radar satellite imagery of locations in Ukraine to Terra Tech; a Russian technology firm that supplies commercially acquired space imagery.[21] Furthermore, the US government reported that the Russian space company Joint Stock Company Research and Production Concern BARL (AO BARL) supports Russia's military operations by sharing foreign high-resolution satellite imagery.[22]

Space enabled imagery is only one source of information; valuable military data is collected through for example surveillance UAVs and human intelligence. All that data needs to be fused and analysed so as to form valuable military intelligence, such as specific targeting information. The conflict in Ukraine demonstrates that open-source intelligence (OSINT), mainly based on commercial satellite imagery and social media like Telegram and YouTube, is increasingly relevant as a complement to traditional military intelligence. Ukraine has benefitted greatly not only from both foreign governmental agencies' intelligence products but also from open sources, leading Russia to declare those commercial satellites to be legitimate targets.[23]

4. Satellite communication (SATCOM)

Russia degraded and partly destroyed the Ukrainian military communications network early in the war. As Ukraine needed a secure communication system to conduct effective defense (e.g. for communication between commanders and frontline troops), Ukraine requested Elon Musk to 'provide Ukraine with Starlink stations.'[24] Starlink, launched by SpaceX in 2019, is a private sector-run, low earth orbit satellite constellation with literally thousands of satellites that provides global high-speed, low-latency broadband internet access. The first Starlink ground terminals arrived within the first week of the conflict and formed a much-needed lifeline. The use of Starlink as a replacement for the Ukrainian command and control system was essential: it allowed the Ukrainian high command to stay on top of developments on the various frontlines.[25] It furthermore enabled connectivity and

[21] U.S. Department of the Treasury, "Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization."

[22] U.S. Department of the Treasury, "Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization."

[23] Bingen, Johnson, and Smith, "Russia Threatens to Target Commercial Satellites."

[24] Sabbagh, "Fury in Ukraine as Elon Musk's SpaceX limits Starlink use for drones."

[25] Economist, "How Elon Musk's satellites have saved Ukraine and changed warfare."

communication with the outside world, e.g. for civilians and combatants trapped in Mariupol, as well as the global distribution of frontline videos and photos via social media. It also allowed President Zelensky to remain in contact with world leaders and the population of Ukraine – all contributing to the mitigation of the Russian (dis)information campaign.[26]

In addition, the Starlink network was used by Ukraine for controlling surveillance UAVs and combat UAVs, such as the Turkish Bayraktar TB2 drone. This became more difficult early this year, when SpaceX tried to prevent such system use. Whilst this offensive use was clear already quite early in the war, Gwynne Shotwell, SpaceX's chief operating officer, declared in February that Starlink was never meant to be weaponised by Ukraine, and that Ukrainians had leveraged it in ways that were not part of any agreement.[27] Even more impactful was the story revealed in Elon Musk's biography. Although the facts are still somewhat unclear, it seems that the Starlink enabled communication was crucial for a planned Ukrainian attack mission with maritime drones. Either Elon Musk (himself) refused to switch on necessary communication covering Sebastopol's harbour to enable the strike on Russian ships responsible for launching missiles into Ukraine, or he switched the crucial communication off. This demonstrates the importance of such systems and the role of commercial actors.

5. Position, navigation, and timing (PNT)

PNT satellites provide positioning data and are used for surveillance, navigation and targeting. Military satellites such as the GPS system are used in Ukraine, as in Iraq in 1991, to aid troops in their routes to supply frontline units and for precise location of targets. Precision weapons are either guided by radio signals, inertial navigation, designated laser or GPS. The latter does not require boots on the ground in the vicinity of the target or continuous observation of the target with e.g. a laser designator to guide ammunitions direct on target whilst minimising collateral damage risk. With the proper codes installed, the accuracy of GPS-guided munitions can be bettered to around one metre. As GPS-guided bombs are 'fire and forget,' the use of it enables the pilot (as most GPS guided bombs are aircraft delivered) to make evasive manoeuvres to disrupt the potential lock-on of anti-aircraft munitions. Artillery (155 mm and High Mobility Artillery Rocket System munitions (HIMARS)-type rocket artillery) are often GPS-guided as well to provide for greater accuracy.

[26] Miller, Scott, and Bender, "UkraineX: How Elon Musk's space satellites changed the war on the ground."

[27] Sabbagh, "Fury in Ukraine as Elon Musk's SpaceX limits Starlink use for drones."

Greater accuracy means that less munition is needed to hit targets as opposed to non-guided artillery and a reduction of collateral damage.

Furthermore, Ukraine receives targeting information from satellites via the United Kingdom and the United States. Undoubtedly, Russia will also generate targeting information from space. However, the number of satellites available to Russia is significantly lower compared to Ukraine and its allies. While Russia has its own space capabilities, such as the Glonass system as a counterpart to GPS, questions remain about its level of precision compared to GPS. The precision of US precision weapons suggests that the combination of Russian comparable weapons and the Glonass signal may not match that of the US. In general, Russia appears to focus more on disrupting Ukrainian space capabilities than deploying its own satellite capacity. Let us turn to those counter space operations now.

6. Space control

The overview above underlines the importance of space technology in this armed conflict and indicates significant strategic advantages. As expected, adversaries have used counter-space capabilities in an attempt to mitigate these advantages. In this section, we first distinguish four types of counter-space capabilities, and then assess which and how these are used in the Russia-Ukraine war.

Presently, various states possess counter-space capabilities, including 1) direct ascent kinetic ASAT missiles (DA-ASAT) and co-orbital interceptors that can physically destroy a satellite; 2) non-kinetic weapons such as lasers to blind or dazzle sensors on satellites, high-powered microwave weapons and electromagnetic pulse (EMP) that can fry its electronics, or nuclear weapons; 3) electronic weapons to jam or spoof the data stream between satellites and their ground stations uplink or downlink;[28] and 4) cyberattacks on space systems and their data.[29] Not only can these attacks take place outside of Earth's atmosphere, but interference with space related infrastructure on Earth is imaginable and probably much easier to conduct.

Although the increasing militarisation and weaponisation raised alarms as to the likelihood of space warfare, no kinetic (irreversible) ASAT weapons have been used so far. Neither DA-ASAT missiles, like the one tested by Russia a few months before the war, nor co-orbital interceptors capable of destroying satellites. There

[28] Electronic weapons disrupt or deny GPS or satellite communication by targeting the electromagnetic spectrum and jamming the data stream or by adding false information to the data stream and so spoofing the signal (e.g. GPS or Satellite phones).

[29] See further Weeden and Samson, *SWF: Global Counterspace Capabilities. An Open Source Assessment*; Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

were co-orbital rendezvous operations, such as Russian inspector satellite Luch, that manoeuvred towards various other satellites to conduct a close proximity operation. However, these satellites were not used as co-orbital ASAT weapons but probably for intelligence gathering.[30] Additionally, there is no reported use of non-kinetic lasers, microwave weapons, or EMP, or nuclear weapons. Despite Russian statements on using Zadira, a powerful laser weapon, its use was neither seen nor confirmed, nor any other directed-energy weapons, such as the Peresvet. But while space control has not taken the form of these two types of counter space capabilities, the other two types are frequent.

A large part of Russian counter space operations consists of electronic attacks. Ukraine also likely deploys such tactics, but there is no mention of this in the regular media. Jamming and spoofing targets the data link between the satellite and the ground station, either disrupting the signal or feeding it with false information. Already before the war, regular GPS jamming hindering UAVs was observed. Right before the invasion, for example, it appeared that an operator temporarily lost control over a Bayraktar drone due to GPS interference, reported to be caused by the Russian electronic weapon Krasukha-4.[31] Russia also attempted to jam the (ground terminals of the) Starlink system and the GPS signal to hinder Finnair's commercial airplanes flying near the Russian exclave of Kaliningrad.[32] Ukraine has also jammed Russian communication, e.g. by consumer radios used for communication between Russian units and their commanders.[33]

Where at the start of the conflict, Russia hampered its own forces almost as much as the opponent's, lessons have been learned.[34] Russia seems to be increasingly successful in the field of electronic warfare.[35] In recent months, leaked Pentagon documents revealed frequent attempts to disrupt the GPS signal for the High Mobility Artillery Rocket System munitions (HIMARS) and that locating and destroying Russian jammers was a high priority for Ukrainian forces.[36] Jamming has also interfered with other smart weapons used by Ukraine, like the Joint Direct

[30] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*, 19.

[31] Bingen, Johnson, and Young, ***CSIS: Space Threat Assessment 2023***, 18; OSCE, "Spot Report 6/2021: SMM long-range UAV unable to take off due to dual GPS signal interference"; Bipindra, "STAR WARS! Russia-Ukraine conflict is world's 1st commercial space war as Moscow's EW tries to cripple Ukraine."

[32] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*, 17.

[33] Höyhtyä and Uusipaavalniemi, "The space domain and the Russo-Ukrainian war: Actors, tools, and impact."

[34] Bronk, "The mysterious case of the missing Russian air force" RUSI, 28 februari 2023

[35] Withington, "Jamming JDAM: The threat to US munitions from Russian electronic warfare."

[36] Marquardt, Bertrand, and Cohen, "Russia's jamming of US-provided rocket systems complicates Ukraine's war effort."

Attack Munitions (JDAMs), negatively impacting their accuracy and causing them to miss targets.[37] A recent RUSI report states that Russian electronic warfare systems, like the Shipovnik-Aero, are increasingly effective and substantially contribute to the large number of destroyed Ukrainian UAVs.[38]

Nonetheless, whilst electronic weapons such as the Krasukha-4 and Shipovnik-Aero pose serious threats, there is no reported use of other sophisticated electronic weapons in Russia's arsenal, such as Synthetic Aperture Radar jamming systems against ISR satellites providing imagery of e.g. Russian troop movements.[39] That is surprising, since these ISR satellites have provided Ukraine with a distinct advantage regarding data and intelligence, as described above.[40] Either the Russian armed forces never quite appreciated their value, were unaware of their location, or lacked the means to act against them.

Other frequently reported counter space operations take the form of cyber-attacks.[41] Right at the start of the war, Russia launched cyberattacks on the ground stations of a space communication system, severely disrupting the communication network of Viasat, a US-founded satellite communications firm. It used 'wiper malware that crashed terrestrial modems via the satellite downlink.'[42] The attack disabled communications of the Ukrainian armed forces, but also wind turbines and internet users across Europe.[43] This seems to have been the most successful cyberattack in the ongoing conflict, and it was one of the reasons why Ukraine needed the Starlink system. Whilst Starlink was under attack from hackers too, it has not been degraded in any significant way. There are indications, however, that Russia might step up its cyber operations, which could raise the threat for space capabilities.[44] And of course, not only Russian hackers are active in this area. Little is known, but Russian satellites, including the national GLONASS system, seem to have been targeted by cyberattacks, either by Ukrainian hackers or those sympathetic to them.[45] Additionally, a Russian military satellite communications

[37] Seligman, "Russia jamming U.S. smart bombs in Ukraine, leaked docs say."

[38] Watling and Reynolds, *RUSI: Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*.

[39] The authors of the CSIS report discuss various potential reasons for this: either these counter space capabilities are in fact deployed but that information is not public, not all the reported Russian capabilities are available or/and as effective as was expected, or they are kept in reserve.

[40] Bipindra, "STAR WARS! Russia-Ukraine conflict is world's 1st commercial space war as Moscow's EW tries to cripple Ukraine"; Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*, 19.

[41] Furthermore, two weeks before the invasion, cyberattacks targeting Ukrainian government systems were observed.

[42] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*, 18.

[43] Weeden and Samson, *SWF: Global Counterspace Capabilities. An Open Source Assessment*.

[44] Sakellariadis and Miller, "Ukraine gears up for new phase of cyber war with Russia."

[45] Odessa Journal, "Ukrainian hackers hacked the Russian Glonass system."

network was subject to a cyberattack and disabled for approximately 24 hours at the end of June 2023. It seems that either a hacking group or even a Wagner affiliated organisation was responsible, as it occurred shortly after the Wagner revolt of June 24.[46] For now at least, space force application in this armed conflict takes the form of electronic and cyberattacks. Whilst analysts assume that Russia has other sophisticated space weapons at its disposal, these have not been used so far. As a result, counter-space operations have disrupted military operations, but not as severe as one might have expected, and it has not turned space into a battleground.

7. Commercial space support

Clearly, space capabilities are no longer exclusively in the hands of armed forces. While the US also used commercial communication services in the First Gulf War, the availability of space capabilities and their level of sophistication have increased tremendously. Companies like SpaceX offer amazingly effective and reliable services. As these networks consist of large constellations of small satellites in low orbit, the system itself is resilient and thus not vulnerable to attacks on single satellites. Computer codes and software are updated easily and quickly, increasing resilience.[47] Furthermore, whilst SpaceX is the most prominent commercial actor, many other companies offer effective military space support. ISR is provided by companies such as Maxar; a capability that was previously reserved for a few armed forces and states. And whilst these are not part of any Ukrainian space program, they are said to be so successful that: 'their combined capability may surpass that of the Russian military.'[48] Clearly, the strategic benefits of space technology are no longer reserved for a few powerful countries with costly military space programs; even smaller countries like Ukraine can now profit from these advantages. This is a clear demonstration that owning assets and capabilities is not required (especially in the space domain) as long as access to their services is provided.

Nonetheless, the involvement of commercial actors and civilians blurs the line between military and non-military actors, leading to two distinct challenges. First, commercial actors can be seen as military targets when they provide military support. Dmitry Rogozin, former director of the Russian Space Agency, suggested that Starlink would not be considered purely civilian anymore, and Dmitry Medvedev,

[46] Menn, "Cyberattack knocks out satellite communications for Russian military."

[47] Miller, Scott, and Bender, "UkraineX: How Elon Musk's space satellites changed the war on the ground."

[48] Hilborne, "What could be the consequences of the Ukraine war in space."

the Deputy Chairman of the Russian Security Council, assumed Starlink satellites to be military objectives and ordered those that were used to guide the attack on the Moskva to be destroyed.[49] Given Russia's ASAT capabilities, it was a serious threat, even more so because many ground stations were provided to Ukrainian civilians. Moreover, civilians increasingly contribute to the war effort. Home built applications, accessible through cellphones and connected through the Starlink network, essentially 'militarised' civilians by allowing them to provide timely intelligence on Russian troops, gathering stations and logistical complexes. It is essential that states are aware of these risks, inform their citizens, and assess whether and how to protect civilians, commercial actors and their systems.

A second challenge to be taken into account is the power and influence of companies supplying critical technology. While initially it appeared that SpaceX helped the Ukrainians by providing the Starlink service at little cost, Musk requested that the Ukrainian government would pay for its use when the network had proven essential, although in the end the US DoD decided to pay the bill.[50] On June 1st this year, the Pentagon disclosed that they had signed a contract purchasing an unknown amount of Starlink terminals from SpaceX. More concerning, this sort of power not only means that companies such as SpaceX can secure lucrative deals, but can also influence geopolitical processes and military operations.[51] The prime example is Elon Musk, who got involved in the politics by proposing peace terms on Twitter and high-level meetings with political and business leaders.[52] Also, the use of commercial space services can be unreliable when the supplier restricts their extended use. SpaceX declared that they did not allow the use of Starlink for offensive purposes, whilst it was being used extensively for communication and targeting. Services were cut back to prevent it from being weaponised and used for guiding combat UAVs.[53]

[49] Ranjan, "Russia announces space war on Elon Musk's Starlink satellites, accepts Moskva was attacked"; DW, "Ukraine updates: US warns Russia over satellites threats."

[50] Belfer Center, "Starlink and the Russia-Ukraine War: A case of commercial technology and public purpose?"; Marquardt, "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab."

[51] The Belfer Center refers to the risk 'when private companies acting in their own capacity do not acknowledge the larger ecosystem of procurement and crisis response. This allows for efficient deployment, but the politics and perception of wartime support are fraught and there are reasons why countries take time to consider what technology and training they can provide.' Belfer Center, "Starlink and the Russia-Ukraine War: A case of commercial technology and public purpose?"

[52] Metz, Satariano, and Che, "How Elon Musk became a geopolitical chaos agent."

[53] Roulette, "SpaceX curbed Ukraine's use of Starlink internet for drones -company president."

8. Conclusion

The armed conflict between Russia and Ukraine demonstrates the importance of space technology for contemporary warfare. It has enabled unprecedented transparency, supported logistics, increased precision in targeting, and has played a key role in exposing enemy locations, potential war crimes, humanitarian crises, and environmental damage. In that way, it has helped Ukraine to effectively defend itself, aided the process of truth-finding and justice, and has contributed to countering Russian censure, propaganda and information operations. Space technology continues to fulfill its role as a critical enabler of modern military operations. However, where the First Gulf War might have been the first 'space war,' this conflict would be the first 'commercial space war.'[54] While Ukraine did not have military satellites before the war, the capabilities provided by other states and commercial actors gave them a significant military advantage.[55]

That also highlights the need for and importance of international cooperation, including with commercial actors. Hybrid space networks can enhance the capability output without having to double existing capabilities or increase budgets for space capabilities, for example by optimising interoperability (also in the field of Space Situational Awareness, where a global network of sensors is necessary), improving data sharing on existing capabilities and threats, and strengthening resilience through a combination of multiple systems. Moreover, the commercialisation of the space domain means that we need to think about the role of the space industry, and how to mitigate challenges related to the risk of companies and civilians getting involved in armed conflicts. The type and degree of responsibility that states have for the safety of those commercial actors and civilians are still unclear at this moment – something that must be addressed as this involvement will only increase in the face of these technological developments. Furthermore, civil-military cooperation requires clear agreements between participating sides as to what is delivered, who is in control, how the costing is arranged, and how the agreed service level can be maintained.

Space did not turn into a 'bloody' battlefield, as some feared. There was no use of kinetic ASAT weapons, laser weapons, and certain advanced electronic weapons – capabilities that Russia was believed to have. Nonetheless, Russian counter space

[54] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

[55] Of the five mission areas generally recognised, in this conflict we mainly see Space Force Enhancement (in SATCOM, ISR and PNT) and Space Control (in counter space activities). Space Situational Awareness (SSA), Space Force Application (SFA) and Space Support have been less in demand as Ukraine is not (yet) a space faring nation limiting the means to conduct operations in these mission areas.

operations continue to pose a serious threat. In the past year, they have been used to 'disrupt command, control, communications, and intelligence gathering and to degrade the effectiveness of UAVs and precision munitions.'[56] Recent developments suggest that they are increasingly successful particularly in electronic warfare.[57] Moreover, the importance of space technology in this conflict will incentivise other states to gear up their counter space capabilities. Given recent developments, a shift in the character of counter space capabilities can be expected. The use of kinetic ASAT weapons is possible but increasingly unlikely: they are relatively expensive, produce space debris,[58] and are ineffective for targeting large constellations. Moreover, the debris itself will likely hamper the perpetrator's use of space as well, which is a great deterrent for conducting such attacks. Other types of counter-space capabilities might thus be more attractive, e.g. more advanced cyber and electronic weapons, kinetic attacks on ground stations, or high-altitude nuclear detonations (HANDS).[59] The use of counter-space capabilities in this armed conflict allows states to draw lessons for space control, and indicates that the focus needs to shift from (countering) kinetic ASAT weapons to (countering) increasingly sophisticated 'soft kill' weapons.

While we need to be careful when drawing lessons from this ongoing and evolving armed conflict, this analysis indicates that space technology is crucially important in modern day warfare, that it continues to be a critical enabler, is essential in multi-domain operations, and that space capabilities have become far more advanced and comprehensive. At the same time, the Russia-Ukraine war makes clear that this goes hand in hand with certain challenges. Most notably, the blurring of the military-civilian lines requires us to rethink the responsibility of states for companies and civilians that contribute to the war effort, pay more attention to effective and balanced public-private partnerships, and prepare for new (and old) threats to space systems.

[56] Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

[57] Robinson, "Ukraine conflict points to a future of space-enabled war."

[58] There is a similarity with nuclear deterrence dynamics: The(first) use of a destructive attack will lead to mutual degradation of capabilities and extreme levels of disruption, to the point where entire orbits will be rendered useless.

[59] See further: Bingen, Johnson, and Young, *CSIS: Space Threat Assessment 2023*.

Lonneke Peperkamp

Lonneke Peperkamp is professor of military ethics and leadership at the NLDA. With a background in law, philosophy, and conflict studies, she focuses in her research on global justice, just war theory, and the ethics of new technologies in warfare, such as space technology, remote warfare, autonomous weapon systems, (cyber-enabled) psychological influencing operations, and soldier enhancement. She is affiliated with the Interdisciplinary Research Hub on Digitalization and Society (iHub, Radboud University Nijmegen) and the Centre of Military Ethics (King's College London). She is vice president of EuroISME, the International Society for Military Ethics in Europe.

Patrick Bolder

Patrick Bolder is a retired LtCol of the Royal Netherlands Air Force after a career of 40 years in Meteorology first and later in several Plans and Policy postings at the Airstaff and Defence Staff. He graduated from Staff College in 2001 and is an alumni of NATO Defence College Senior Course 125 in 2014. He made two tours (2012 and 2017) in the United States Security Coordinator (USSC) mission, working in its British Support Team based in Ramallah, serving as Military Technical Advisor Training for the Palestinian General Military Training Commission in Jericho and Ramallah. At the end of his military career he was seconded to the Hague Centre for Strategic Studies think tank. His current fields of expertise are unmanned systems, military use of space, and defence planning.

Bibliography

Anson, Peter, and Dennis Cummings. "The First Space War: The Contribution of Satellites to the Gulf War." *The RUSI Journal* 136, no.4 (1991): 45-53. https://doi.org/10.1080/03071849108445553.

Belfer Center. "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" *Belfer Center for Science and International Affairs, Harvard Kennedy School*, March 9, 2023. https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

Bingen, Kari, Kaitlyn Johnson, and Zhanna Smith. "Russia Threatens to Target Commercial Satellites." *Center for Strategic and International Studies*, November 10, 2022. https://www.csis.org/analysis/russia-threatens-target-commercial-satellites.

Bingen, Kari, Kaitlyn Johnson, and Makena Young. *Space Threat Assessment 2023*. Washington D.C.: Center for Strategic and International Studies, 2023.

Bipindra, N.C. "STAR WARS! Russia-Ukraine Conflict Is World's 1st Commercial Space War As Moscow's EW Tries To Cripple Ukraine." *EurAsian Times*, April 23, 2023. https://www.eurasiantimes.com/star-wars-russia-ukraine-conflict-is-worlds-first-commercial/.

Browne, Malachy, David Botti, and Haley Willis. "Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims." *New York Times*, April 6, 2022. https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html.

Caldicott, Helen, and Craig Eisendrath. *War in Heaven: The Arms Race in Outer Space*. New York: The New Press, 2007.

DW. "Ukraine Updates: US Warns Russia over Satellites Threats." *DW*, October 27, 2022. https://www.dw.com/en/russia-ukraine-updates-us-warns-russia-against-targeting-wests-satellites/a-63570741.

Economist. "How Elon Musk's Satellites Have Saved Ukraine And Changed Warfare." *Economist*, January 5, 2023. https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

Erwin, Sandra, and Debra Werner. "Dark Clouds, Silver Linings: Five Ways War in Ukraine Is Transforming the Space Domain." *Space News*, December 23, 2022. https://spacenews.com/dark-clouds-silver-linings-five-ways-war-in-ukraine-is-transforming-the-space-domain/.

Friend, Cody. "Space Force's First Targeting Squadron Brought to Life." *DVIDS*, August 11, 2023. https://www.dvidshub.net/news/451367/space-forces-first-targeting-squadron-brought-life.

Hilborne, Mark. "What Could Be the Consequences of the Ukraine War in Space?" *King's College London*, March 10, 2022. https://www.kcl.ac.uk/what-could-be-the-consequences-of-the-ukraine-war-in-space.

Marquardt, Alex, Natasha Bertrand, and Zachary Cohen. "Russia's Jamming of US-provided Rocket Systems Complicates Ukraine's War Effort." *CNN*, May 6, 2023. https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html.

Menn, Joseph. "Cyberattack Knocks Out Satellite Communications for Russian Military." *Washington Post*, June 30, 2023. https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/.

Metz, Cade, Adam Satariano, and Chang Che. "How Elon Musk Became a Geopolitical Chaos Agent." *New York Times*, October 26, 2022. https://www.nytimes.com/2022/10/26/technology/elon-musk-geopolitics-china-ukraine.html.

Miller, Christopher, Mark Scott and Bryan Bender. "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground." *Politico*, June 8, 2022. https://www.politico.eu/article/elon-musk-ukraine-starlink/.

Odessa Journal. "Ukrainian Hackers Hacked the Russian GLONASS System." *Odessa Journal*, February 6, 2023. https://odessa-journal.com/public/ukrainian-hackers-hacked-the-russian-glonass-system.

OSCE. "Spot Report 6/2021: SMM Long-Range UAV Unable to Take Off Due to Dual GPS Signal Interference." *Organization for Security and Co-operation in Europe*, April 7, 2021. https://www.osce.org/special-monitoring-mission-to-ukraine/483008.

Ovsyaniy, Kyrylo. "Satellite Images Reveal How Russia's Invasion Has Devastated The Environment In Ukraine." *RFE/RL*, March 5, 2023. https://www.rferl.org/a/ukraine-satellite-photos-environmental-damage-russia-invasion/32300056.html.

Ranjan, Rohit. "Russia Announces Space War On Elon Musk's Starlink Satellites, Accepts Moskva Was Attacked." *Republic World*, April 16, 2022. https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-announces-space-war-on-elon-musks-starlink-satellites-accepts-moskva-was-attacked-articleshow.html.

Robinson, Tim. "Ukraine Conflict Points To a Future of Space-Enabled War." *Royal Aeronautical Society*, June 14, 2022. https://www.aerosociety.com/news/ukraine-conflict-points-to-a-future-of-space-enabled-war/.

Roulette, Joey. "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones -Company President." *Reuters*, February 9, 2023. https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.

Sabbagh, Dan. "Fury in Ukraine As Elon Musk's SpaceX Limits Starlink Use for Drones." *Guardian*, February 9, 2023. https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk.

Sakellariadis, John, and Maggie Miller. "Ukraine Gears Up for New Phase of Cyber War with Russia." *Politico*, February 25, 2023. https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429.

Shaw, John. "Welcome to the Third Space Age." *Space News*, August 29, 2023. https://spacenews.com/op-ed-welcome-to-the-third-space-age/.

Seligman, Lara. "Russia Jamming U.S. Smart Bombs in Ukraine, Leaked Docs Say." *Politico*, April 12, 2023. https://www.politico.com/news/2023/04/12/russia-jamming-u-s-smart-bombs-in-ukraine-leaked-docs-say-00091600.

Steer, Cassandra, and Dale Stephens. "Applying International Humanitarian Law in Outer Space." In *War and Peace in Outer Space. Law, Policy, and Ethics*, edited by Cassandra Steer and Matthew Hersch, 23-54. New York: Oxford University Press, 2021.

Tingley, Brett. "US Space Force Creates 1st Unit Dedicated to Targeting Adversary Satellites." *SPACE.com*, August 16, 2023. https://www.space.com/space-force-1st-targeting-squadron.

Ukrinform. "'People's Satellite' Helps Spot Thousands of Units of Russian Equipment." *Ukrinform*, September 3, 2023. https://www.ukrinform.net/rubric-ato/3680266-peoples-satellite-helps-spot-thousands-of-units-of-russian-equipment.html.

U.S. Department of the Treasury. "Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization." *U.S. Department of the Treasury*, January 26, 2023. https://home.treasury.gov/news/press-releases/jy1220.

Watkins, Ronald. "Finnish Company to Provide Ukrainian Army With Satellite Imaging." *The Defense Post*, August 19, 2022. https://www.thedefensepost.com/2022/08/19/finnish-company-ukraine-satellite-imaging/.

Watling, Jack, and Nick Reynolds. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* London: Royal United Services Institute, 2023.

Weeden, Brian, and Victoria Samson. *Global Counterspace Capabilities: An Open Source Assessment*. Washington D.C.: Secure World Foundation, 2020.

Withington, Thomas. "Jamming JDAM: The Threat to US Munitions from Russian Electronic Warfare." *Royal United Services Institute*, June 6, 2023. https://www.rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare.

Zwanenburg, Marten, Lonneke Peperkamp, and A. Siemensma. "De Russische antisatellietwapentest: Onverantwoordelijk maar (nog) niet illegaal?" *Nederlands Juristenblad* 97, no.7 (2022): 487-493. http://deeplinking.kluwer.nl/?param=00DA5DAB&cpid=WKNL-LTRNav2.