Proliferation of Satellite Mega-Constellations: Strategic Security and Defence Implications for the European Union

1. Introduction

Since the early 2010s, the space industry has undergone a significant transformation. The traditional dominance of government agencies in the sector has been challenged by the emergence of private U.S. companies such as SpaceX and Blue Origin, focused on developing innovative, low-cost space technology. This trend towards commercialisation has spread outside the United States, as countries such as China and India are increasingly investing in private space enterprises to develop their space capabilities (Pelton & Madry, 2020). Most notably, the privatisation of the space sector has fostered a reduction in space launch costs through technological advancements such as reusable rockets, cheaper manufacturing processes, and satellite miniaturisation (Young & Thadani, 2022).

Today's expanded access to space is enabling the deployment of large networks of thousands of satellites in low earth orbit (LEO). Referred to as LEO constellations, such satellite systems are designed to provide high-speed internet across the globe (Hallex & Cottom, 2020). Perhaps the most well-known example is SpaceX's Starlink, an LEO constellation famous for its unprecedented commercial success. Although SpaceX is the only operator to offer broadband satellite internet to the consumer market as of 2024, numerous governments and private companies are racing to establish their own alternative service. In this context, the number of proposals for LEO constellations has grown considerably in the past few years, the most prominent of which include OneWeb, project Kuiper, LEO Lightspeed, and China's Guowang.

Beyond mass-market connectivity, LEO satellite constellations demonstrate a significant potential for security and defence applications and could confer strategic advantages to their operators (Young & Thadani, 2022). Their proliferation therefore introduces new security and defence implications globally. Given the recent nature of these developments, academic literature about LEO constellations largely focuses on digital development, international security, and US national security implications. However, proliferated LEO constellations are also particularly relevant to the EU. In the current context of space militarisation and power competition between China, the US, and Russia, the bloc is facing pressure to develop autonomous security and defence capabilities in space, improve its launch capabilities, and protect its space assets from external threats (Council of the European Union, n.d). Within this scope, the following question is addressed: What are the implications of the proliferation of LEO satellite constellations for EU strategic autonomy in security and defence?

This article begins with a background chapter before examining several constellations in development and their applications. The focus is first set on SpaceX's Starlink and US military LEO constellation programs. It then shifts to major LEO projects in China. Finally, these cases are

analysed in relation to the EU's space capabilities, highlighting the overall implications for EU strategic autonomy in security and defence.

2. Background

2.1 Basics of Satellites

Before discussing the strategic relevance of LEO constellations, this section explains the basic technicalities of satellites. Since the launch of Sputnik 1 in 1957, various actors have deployed artificial satellites in orbit around Earth to perform specific missions. These missions typically fall into one of three categories, which are communications, observation, or navigation. Communications missions provide radio, television, phone, or internet services. Earth observation missions collect measurements and images of the Earth's surface. Meanwhile, navigation missions enable users on the ground to determine their location. Because a single satellite can only cover a limited area of the Earth, satellites often operate in groups known as constellations. These configurations make it possible to undertake missions with global coverage from a given orbit (CBO, 2023; Voelsen, 2021).

Satellites are usually launched into one of three main orbits: Low Earth orbit (LEO), at an altitude of 160 to 2000 km, Medium-Earth Orbit (MEO), from 2000 km to 35,786 km, and Geostationary Earth Orbit (GEO), at 35,786 km. LEO and MEO satellites are in constant motion relative to the surface. In particular, LEO satellites circle the earth multiple times per day, staying in view of a given location for about 10 minutes. In contrast, GEO satellites remain permanently fixed above the same ground location by matching the earth's 24-hours rotation period (Figure 1) (CBO, 2023). Due to their larger field of view and their ability to deliver continuous coverage, GEO satellites are ideal for observation or broadcasting over large areas. Typically, a GEO constellation of only 4 satellites is needed to provide global coverage, ensuring lower launch and operating costs. For this reason, GEO satellites have been predominant in communications for the past 50 years. However, their high altitude means that signals take longer to travel from the earth and back, resulting in a longer latency. MEO satellites, as they stand, are prevalent in navigation missions as they can provide stronger signals across different earth latitudes (CBO, 2023; Young & Thadani, 2022). Lastly, LEO satellites are now being explored for several applications, as we will see shortly.

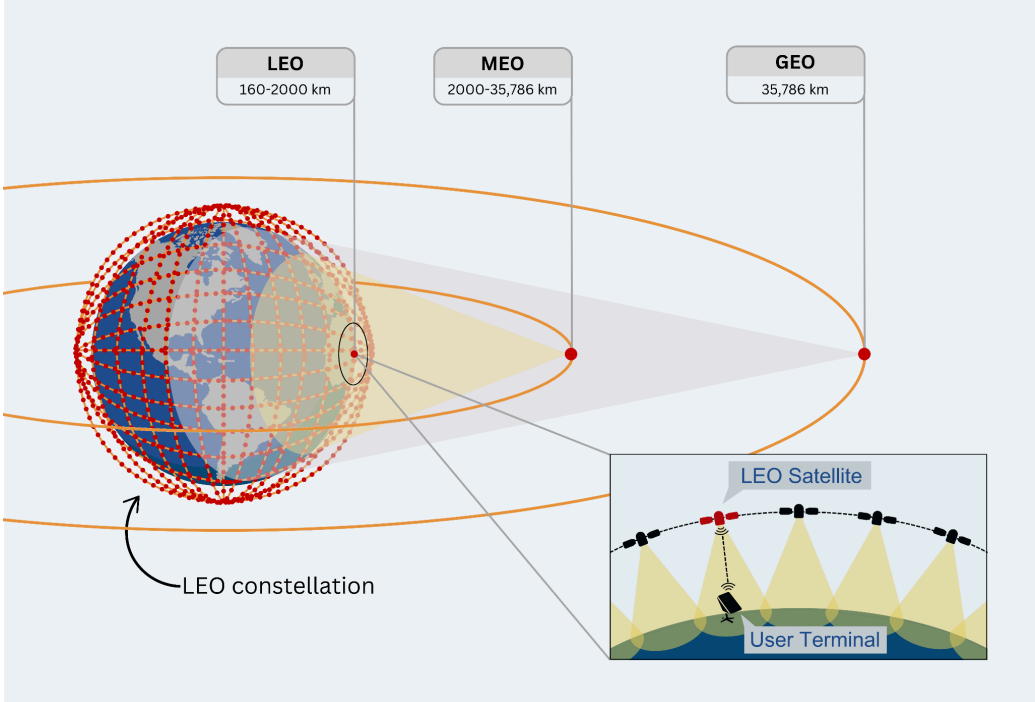

Figure 1: Orbits and LEO Constellations (own work)

2.2 Satellites as Critical Infrastructure and Key Defence Assets

Over the years, satellite services have become essential for numerous societal functions such as aviation, maritime traffic, weather forecasting, agriculture, government communications, search and rescue, and broadcasting. The indispensable role that they exert in maintaining the functionality of other systems and societal functions places satellites in the category of critical infrastructures (CIs). As such, they are increasingly included in special national protection frameworks to safeguard national security (Froehlich, 2021; Schrogl, 2020).

It is important to distinguish between national security, which largely describes the ability of a state to protect its citizens from various threats, and defence, a specific aspect of national security focused on protecting the nation from external military threats (Osisanya, n.d.). Satellites have also long fulfilled defence applications, including providing secure military communications, navigation, targeting guidance, and perhaps most famously, reconnaissance. Reconnaissance satellites may monitor enemy military activities, intercept foreign communications, and detect ballistic missiles (Pelton & Madry, 2020).

2.3 Proliferation of LEO Mega-Constellations in the Age of Commercial Space

Breaking with the traditional dominance of GEO satellite systems in satellite communications, a growing number of companies are now developing LEO satellite constellations to provide global broadband internet services. As of 2023, around 33 percent of the global population remained

offline, largely due to the lack of internet access in rural areas and least-developed countries (ITU, 2023). This digital divide is attributed to the limited coverage of ground-based internet infrastructure and GEO internet satellites. Despite handling the majority of global internet traffic, ground-based infrastructure is challenging and expensive to build in remote areas. Conversely, GEO satellites can transmit internet signals directly from orbit but are limited by low speed, high latency, and high service prices (Young & Thadani, 2022).

Capitalising on mass-market appeal and economies of scale, LEO constellation operators intend to make significant profits by offering affordable, high-quality internet in underserved areas. Thanks to their low orbital altitude, LEO constellations can provide global coverage with download speeds reaching up to 250 megabits per second (Mbps), and as low as 25 milliseconds of latency – compared to 600 milliseconds for GEO satellites- (Starlink, n.d; Young & Thadani, 2022). However, because individual LEO satellites cover a smaller area, achieving similar coverage in LEO requires a significantly larger number of satellites (Figure 1). For instance, the Starlink constellation comprised more than 6000 satellites in September 2024 (Pultarova et al., 2024;). Due to their sheer scale, LEO constellations are often referred to as "mega-constellations" (Hallex & Cottom, 2020). Satellites are linked to one another using lasers, while user terminals on the ground continuously connect with the nearest passing satellite (Satariano et al., 2023).

The deployment of such large constellations today has been made possible by a combination of recent developments in the commercial space sector. From the 2000s, the emergence of a new US private aerospace industry known as NewSpace has set focus on developing low-cost space technology and improving access to space. Led by companies such as SpaceX and Blue Origin, NewSpace has brought about an increased number of launch providers and more efficient launch vehicles like the reusable Falcon 9 rocket, driving down the costs of space launch. (Pelton & Madry, 2020; Young & Thadani, 2022). A similar development of the commercial space sector is occurring outside the US, as nations like China are increasingly investing in private space enterprises to develop their own space industries. Reflecting these trends, the number of proposals for mega-constellations has grown considerably in the past few years (Figure 2).

Beyond providing commercial internet service, LEO constellations hold significant potential for security and defence applications. Their Broadband capabilities enable the provision of timely military communications in any location worldwide and the relay of large amounts of intelligence data. If outfitted with specific satellite payloads, LEO constellations could also perform enhanced global remote sensing and missile detection tasks. Above all, their large numbers of easily replaceable satellites increase resilience against attacks. (Young & Thadani, 2022; Pelton & Madry, 2020). In light of the strategic advantages that LEO constellations could confer to nations and private entities that deploy them, their proliferation introduces new security implications globally.

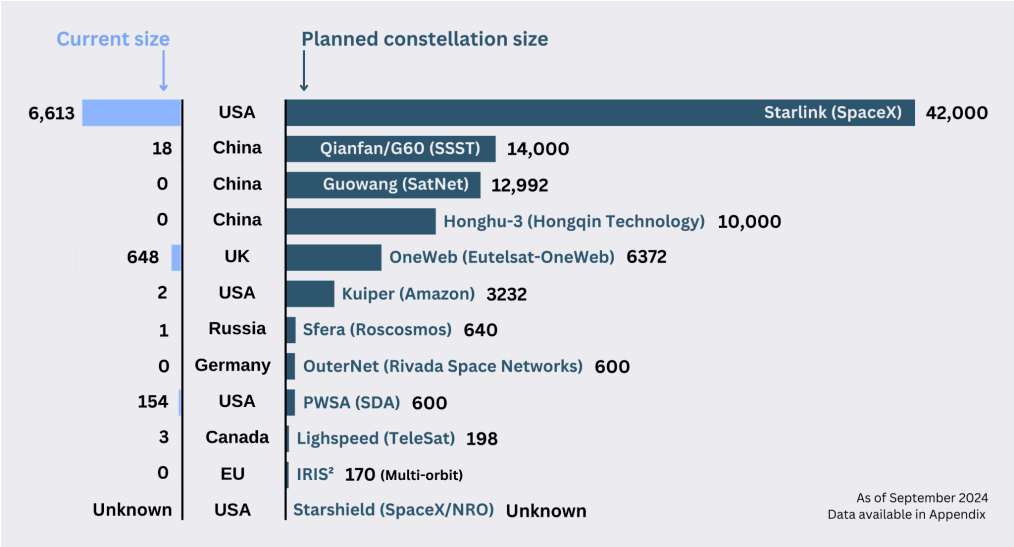

Figure 2: Current LEO Constellations in Development (own work, layout inspired by Voelsen (2021))

2.4 The Relevance of the Space Domain and LEO Constellations for EU Strategic Autonomy

Exemplified by the proliferation of LEO mega-constellations, rapid developments in the space domain have prompted reactions from the European Union in recent years, positioning EU space policy as an important element for achieving strategic autonomy. The concept of EU strategic autonomy widely describes the ability of the union to act autonomously and protect its interests in diverse sectors such as trade, foreign policy, technology, defence, and security without being restrained by dependencies on foreign actors (Helwig & Sinkkonen, 2022; Zhang et al., 2022).

Today, space has become increasingly relevant to EU strategic autonomy within the fields of security and defence for several reasons. Since space infrastructures like satellites are essential enablers for numerous societal functions and military activities, developing homegrown space assets is critical to ensure autonomous security and defence capabilities. For instance, the existing Galileo MEO constellation provides an independent navigation system for civil and military applications, reducing member states' reliance on the US's GPS, Russia's GLONASS, or China's Beidou systems (Cellerino, 2023; Radhakrishnan et al., 2016). Besides, the current geopolitical context of power competition between China, the US, and Russia – which each possess anti-satellite (ASAT) weapons – is fueling a race to develop advanced military capabilities in space. Lastly, the EU still lacks effective launch capabilities and risks being increasingly dependent on external actors for its access to space (Harrison, 2024; Küsters et al., 2024; UN, 2023). Overall, these developments are pressuring the union to develop its security and defence capabilities in space, improve its launch capabilities, and protect its space assets from external threats.

To this end, the European Commission and the High Representative introduced the first-ever EU space strategy for security and defence in March 2023. Among others, the joint communication calls for the development of new EU launchers to ensure autonomous access to space. It also mentions the commission's intent to exploit upcoming LEO constellations for military capabilities. Crucially, it sets as an objective the deployment of IRIS², a sovereign multi-orbit constellation (Council of the European Union, n.d.; European Commission, 2023). These measures suggest that the bloc is carefully considering the global proliferation of mega-constellations as it lays down its plan for achieving strategic autonomy.

Against this backdrop, this article unravels the various implications that the said proliferation holds for EU strategic autonomy in security and defence. The subsequent sections discuss different LEO constellation initiatives and assess how they may impact the EU's ability to act autonomously and protect its interests in the two fields. The decision to focus on constellations from the US and China stems from the fact that both countries are currently at the forefront of LEO mega-constellations development (Figure 2). Moreover, the current debate on EU strategic autonomy is driven by the growing rivalry between the two geopolitical powers, which exposes the EU to security challenges and limits its ability to implement its foreign policy (Helwig & Sinkkonen, 202).

3. Discussion

3.1 Starlink and US Military Constellations

SpaceX's Starlink is the first commercially successful LEO mega-constellation. By May 2024, it provided high-speed internet to more than three million customers in 99 countries worldwide (Alvarez, 2024). Users connect to the constellation through a small terminal that can be set up in minutes and managed via an app.

Far ahead of any competitor on the market, Starlink's unique capabilities have proven groundbreaking in critical civilian and military applications throughout the Russo-Ukrainian war. SpaceX dispatched thousands of Starlink terminals to Ukraine shortly after the start of the invasion to restore connectivity where Russian troops had disabled telecommunication infrastructure (phone lines, cell towers, ground stations, fibre optic lines, and broadcasting antennas) (Bergengruen, 2022; Jayanti, 2023). Thanks to its independence from ground infrastructure, Starlink's service has remained unaffected by Russian attacks. Moreover, its low-cost and user-friendly hardware has allowed for easy adoption and deployment while its high number of satellites and terminals has rendered jamming particularly challenging. Lastly, such advantages have been further compounded by high-speed, low-latency connection, portable and compact terminals, and remote connectivity capabilities (Jayanti, 2023; Kaushik & Selvamurthy, 2023).

This combination of features fostered a swift adoption of the satellite service in hospitals, aid organisations, schools, and businesses (Jayanti, 2023). Above all, Starlink was adopted by the Ukrainian military, enabling real-time communication between command centres and frontline units operating in areas lacking telecommunications. Ukrainian units have also commonly used Starlink's broadband to deploy a large number of drones over vast swathes of territory, performing reconnaissance missions and dropping explosives on enemy positions (Wiedemar, 2023; Davis, 2022). Besides the growing use of autonomous systems, the conflict has seen an increase in the processing of battlefield intelligence. Large amounts of data – including satellite images and GPS coordinates of Russian troops – have been shared by earth observation companies through Starlink's broadband connection and fed into military software providing intelligent battlefield management. For instance, the software GIS Arta coordinates Ukrainian artillery strikes based on field information. Kyiv also relies on Palantir's Metaconstellation, an AI software that detects military targets and predicts their movements from satellite images (Giles, 2023; Wiedemar, 2023).

Russia's continued targeting of communication infrastructure has reportedly made Starlink the only internet service left in Ukraine. With some 42,000 terminals in use in the region, it has become vital for Ukrainian military operations and civilian life (Abels, 2024; Reuters, 2024). This dependency has raised concerns about Ukraine's sovereignty over its military capabilities, considering that Starlink is controlled by SpaceX, a private company owned by US billionaire Elon Musk. Notably, SpaceX has continuously disabled Starlink service in Russian-occupied areas and outside Ukrainian borders using geofencing. In February 2023, it imposed further restrictions on usage for offensive military purposes such as drone control (Abels, 2024; Giles, 2023). These restrictions have hampered Ukrainian efforts to retake territory and contributed to the freezing of the conflict. Although the aerospace company has justified its service restrictions as a response to Starlink's unanticipated weaponisation violating its terms of service, its motives as a private actor remain opaque. Indeed, the company may have been aiming to avoid becoming a party to the conflict following Russian threats of ASAT retaliation against private space infrastructure supporting Ukraine (Abels, 2024; Boley & Byers, 2024; Giles, 2023; Wiedemar, 2023).

Dependence on Starlink as a critical communication infrastructure is not limited to Ukraine. The constellation has become essential in Brazil's Amazon region, where it operates 70,000 terminals in more than 90% of municipalities. There, isolated communities, schools, hospitals, and even illegal mining compounds rely on its extensive broadband coverage for their communications. Moreover, the Brazilian Ministry of Defence has recognised Starlink as key to Brazil's defence operations. The service is indeed used by the military for command and control, particularly in communicating with remote bases and border platoons (Alvarez, 2023; Phillips & Milmo, 2024). Such a situation is problematic for Brazil's national security given the considerable leverage granted to a private company.

To mitigate reliance on private infrastructure such as Starlink for defence, the US Space Force's Space Development Agency (SDA) is deploying its own LEO military constellation while maintaining collaboration with the commercial sector. Known as the Proliferated Warfighter Space Architecture (PWSA), the satellite network is set to consist of different layers, including a tracking layer for remote sensing and missile warning, and a transport layer providing high-speed communications and battlefield management. The transport layer will be capable of connecting to private constellations for third-party services while maintaining control over operations (Abels, 2024; Young & Thadani, 2022). Furthermore, the US National Reconnaissance Office (NRO) contracted SpaceX in 2021 to develop Starshield, a military LEO constellation designed specifically for global remote sensing and defence communications (Roulette & Taylor, 2024; SpaceX, n.d.). Establishing efficient satellite services in LEO thus appears to be a priority for the US as it seeks to become a dominant military power in space.

Figure 3: Ukrainian Soldier Setting Up a Starlink Terminal (Attribution: Mil.gov.ua)

3.2 China's Answer to Starlink

While Starlink's recent success has occupied the spotlight, interest in LEO constellations extends beyond the United States. China, in particular, has been pursuing its own LEO constellation projects to provide global broadband internet access. In March 2020, the Chinese government announced plans to launch a constellation named Guowang. Managed by the state-owned China Satellite Network Group (SatNet), it will consist of 12,992 satellites in LEO (Suess, 2023; Young & Thadani, 2022). Guowang is one of three main Chinese mega-constellation projects as

of September 2024, alongside Qianfan (“Thousand Sails”, previously G60) and Honghu-3. Qianfan, Led by Shanghai Spacecom Satellite Technology and supported by Shanghai’s municipal government, launched the first 18 of its 14,000 planned satellites in August 2024. Honghu-3, led by Hongqing Technology, aims to deploy 10,000 satellites at term (Jones, 2024; Page, 2024). These initiatives receive significant support from the Chinese Communist Party and benefit from the rapid development of China's commercial space sector, which is expected to deliver the necessary growth in launch capacity to deploy thousands of satellites into space.

China may have several motives for financing LEO constellation projects, one of them being the commercial opportunity these offer. Despite its success, Starlink is awaiting government approval to operate in dozens of countries across Africa, Central Asia, and South Asia, and is unavailable in Syria, Russia, China, Iran, Afghanistan, Belarus, and North Korea (Starlink, n.d.). SpaceX’s satellite service has faced criticism from authoritarian regimes for bypassing the traditional ground-based infrastructure that they control to censor information (Satariano et al., 2023). As such, several governments hesitate to authorise its operation within their borders, preferring to maintain tight control over internet access. These circumstances present an opportunity for Chinese constellations to introduce competing services on the international market. Indeed, China is known for conducting business with authoritarian regimes, but also with emerging markets as part of its Belt and Road Initiative (BRI) (Hallex & Cottom, 2020). BRI programs such as the Digital Silk Road (DSR) assist member states in developing their communications infrastructure. Under the BRI’s Space Information Corridor, Beijing has signed over 117 space cooperation agreements with more than 37 governments to share its space infrastructure and provide communication services. (Young & Thadani, 2022). Today, a substantial part of the digital infrastructure in several BRI countries is Chinese-built. This is particularly true in Africa, where Huawei has built an estimated 70% of the continent’s 4G infrastructure (Suess, 2023). For compatibility reasons, these countries may find it easier and more cost-efficient to integrate Chinese LEO Broadband services into their existing network. Concurrently, further BRI agreements could help Chinese LEO broadband providers secure markets in Africa, Asia, and Latin America, potentially pushing out Western providers (Suess, 2023).

Beyond securing China’s position in the satellite internet market, this strategy could serve its soft power interests. Beijing has previously provided several DSR countries with digital surveillance technologies to enhance their online censorship capabilities. In addition, the use of Chinese-built digital infrastructure comes with regulatory compliance requirements, often causing recipient countries to adopt Chinese data governance practices and restrict their social media landscape (Young & Thadani, 2022). The emergence of Chinese LEO constellations as internet suppliers could amplify the dependency of BRI countries on Chinese ICT technologies, exacerbating these trends. A Chinese state-backed satellite internet service with centralised infrastructure would enable client governments to more easily monitor information within their

country's borders and filter politically sensitive content. It could also further spread China's authoritarian internet governance model, as countries seeking access to satellite broadband connectivity might be pressured into aligning with regulatory requirements and censoring content critical of China (Page, 2024; Young & Thadani, 2022). Eventually, a successful proliferation of Chinese LEO broadband constellations could grant China greater control over global information flows and improved intelligence capabilities.

As China seeks to assert its power in the space sector, its military has noted the strategic significance of LEO constellations (Young & Thadani, 2022). Considering the Chinese government's tendency to integrate civilian and military resources, constellation projects such as Guowang or Qianfan constitute likely candidates for providing military capabilities like global high-speed communication and surveillance (Hallex & Cottom, 2020). At the same time, the superpower has sought to prevent Taiwan from acquiring LEO broadband internet. In 2023, Taipei began pursuing such services to safeguard its information infrastructure and ensure connectivity in case of Chinese invasion. This came after Chinese vessels were accused of damaging two undersea cables supplying internet to the Matsu islands, isolating their residents. Subsequent talks with SpaceX to access Starlink were ended by concerns that Elon Musk might face economic pressure from Beijing to shut down the service on request, and Taiwan eventually turned to British operator Eutelsat OneWeb (Khalaf, 2022; Satariano et al., 2023).

Figure 4: Launch of a Chinese Long March 6A rocket - The Same Launcher Model Was Used to Send the First 18 Qianfan Satellites in Orbit on August 6, 2024 (Attribution: ecns.cn)

3.3 Strategic Implications for the European Union

As illustrated by the discussed cases, the emergence of proliferated LEO constellations introduces new sets of opportunities and risks that may impact the ability of the EU to act autonomously and protect its interests in security and defence. Unlike the United States and China, the EU currently lacks the necessary launch capabilities offered by cost-effective, heavy-lift, and reusable launchers to deploy large constellations in LEO. For context, in 2023, the US achieved the world's highest launch rate at 109 launches, 90% of which were conducted by SpaceX. China followed with 67 launches, while the EU recorded only 3 (Kuhr, 2024). Looking ahead, the bloc risks being increasingly reliant on foreign launch providers if it does not improve its independent access to space.

If the EU fails to deploy a sovereign LEO constellation, it risks becoming reliant on non-EU constellations for critical security and defence applications. As observed with Starlink in Ukraine and Brazil, dependence on private infrastructure can undermine sovereignty and national security. Satellite operators obtain significant political leverage, which could limit the EU's ability to enact its policies. Moreover, decisions made by corporate executives like Musk can arbitrarily affect the availability of internet services, threatening the reliability of the communication infrastructure. A private operator could also influence EU common security and defence policy by moderating or shutting down its satellite services in conflict zones depending on the threat posed to its assets. Similarly, relying on future US state-owned LEO constellations such as PWSA and Starshield would perpetuate a situation of dependence on the superpower for military capabilities. Decisions upon service provision would likely be taken by Washington, and the EU may be pressured to align with US foreign policy goals. Currently, this deadlock is well illustrated by Ukraine's extreme reliance on Starlink and by the lack of alternative European LEO internet services to independently counter regional security threats such as Russia's invasion of Ukraine. The invasion also pointed out the growing military importance of space systems and LEO constellations, particularly for AI-enabled battlefield management. This trend is turning space into a warfighting domain as satellites are becoming more relevant targets for retaliation (Davis, 2022). Given its reliance on a small number of satellites highly vulnerable to ASAT weapons, EU space infrastructure is exposed to heightened threats it is not equipped to face.

The proliferation of Chinese LEO constellations brings yet another negative prospect for EU strategic autonomy. If China integrates its future constellations with the BRI and DSR, it could exert greater influence over international communication networks, fostering the spread of its authoritarian internet governance model. China's increased involvement in the field of communications has already sparked security concerns in the EU. A lengthy debate on the integration of Chinese-built equipment in European 5G infrastructure started in 2018 following US allegations that the Chinese government could obtain backdoor access to Huawei and ZTE networks. Eventually, several EU countries restricted or banned telecom equipment from the

two vendors (Cerulus, 2020; Reuters, 2023). Currently, Czechia, Hungary, Poland, and Estonia participate in the DSR and have received Chinese investments in digital infrastructure (Council on Foreign Relations, n.d.). As the EU faces high demand for broader, affordable broadband coverage, alternative offers to Starlink could expose the bloc to a similar dilemma as with 5G infrastructure, possibly compromising its connectivity network.

Brussels seems well aware of the challenges presented by foreign-proliferated LEO constellations. In November 2022, it initiated a program to deploy the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), a sovereign communication constellation. The constellation is planned to have 170 satellites following a multi-orbit architecture (GEO, MEO, and LEO) operable with other systems. Developed via a public-private partnership, the program will involve Airbus, SES, Eutelsat, Hispasat, and Thales Alenia. The consortium is expected to contribute €3 billion of an estimated €6 Billion total cost, splitting investments and benefits between the EU, member states, and private companies (ESPI, 2022; European Commission, n.d.; SES, 2023). Embracing a dual-use approach, IRIS² will in turn deliver high-speed, low-latency secure internet to both governmental and commercial users. On the one hand, it will support border surveillance, crisis management, military missions, and connectivity in key infrastructures such as EU embassies. On the other hand, it will provide internet to EU citizens and private businesses for mass-market applications. With a full constellation planned for 2027, IRIS² constitutes a limited yet strategic response to current LEO constellation projects (European Commission, n.d.; EUSPA, 2024).

Although the completion of IRIS² remains uncertain, developing a sovereign LEO constellation and leveraging commercial LEO services offers opportunities to strengthen the EU's strategic autonomy. As seen in Ukraine, an important benefit of Starlink-like systems is their ability to maintain connectivity when ground infrastructure is damaged. Presently, 95% of global internet traffic between regional networks goes through a network of high-performance undersea cables. This backbone transmits everything from financial transactions to encrypted government communications (Runde et al., 2024). Despite their strategic importance, subsea cables lie highly exposed to accidental damage and sabotage on the ocean floor. Russia has shown a willingness to exploit this vulnerability to disrupt Western communications and Russian vessels have previously been suspected of sabotage in the Baltic Sea (Page, 2023). This is especially concerning for the EU, which relies on Atlantic undersea cables to access a significant portion of its data stored in US data centres (Wall & Morcos, 2021). In this context, a constellation such as IRIS² could complement cable-based internet, providing a contingency to the EU in case of damage to its ground infrastructure (Hallex & Cottom, 2020).

Most importantly, the EU has long sought to build up its military capabilities through initiatives for defence cooperation and industry innovation. The invasion of Ukraine has raised awareness about European defence and has seen Many member states increasing their defence budget and investing in new technologies (EDA, 2024). Within this scope, the deployment of

homegrown LEO constellations is particularly relevant. The powerful impact of Starlink in Ukraine demonstrates that such systems can work as force amplifiers, increasing the resilience of critical infrastructure and the effectiveness of military operations. In turn, they further demonstrate a potential to strengthen the EU's strategic autonomy.

4. Conclusion

Today, the majority of low earth orbit constellation projects remain in the early stages of development. But while the United States and SpaceX enjoy a significant head start with Starlink, the emergence of other constellations is set to empower upcoming operators, be it governments or private companies. Indeed, such space systems promise not only to redefine the connectivity landscape by providing worldwide broadband internet service but also hold significant potential for security and defence applications. Their development is therefore of significant relevance for the European Union, which faces a pressing need to improve its autonomous defence capabilities, develop its space launch sector, and protect its space assets from external threats. The proliferation of Low Earth Orbit (LEO) constellations thus introduces new opportunities and risks that may impact the bloc's capacity to act autonomously and protect its interests in security and defence.

Above all, if the EU fails to deploy a sovereign constellation, it risks becoming reliant on non-EU systems for critical security and defence applications. Relying on a private constellation like Starlink, whose service is subject to moderation, or a foreign state-owned one such as the US-planned Proliferated Warfighter Space Architecture (PWSA), would threaten the reliability of communications and the ability of the EU to enact independent policies and operations. Another negative prospect for EU strategic autonomy comes with the proliferation of Chinese LEO constellations. Through integration with the Belt and Road Initiative and Digital Silk Road programs, these systems could give China greater control over international data flows. Possible integration of CCP-backed LEO broadband services into the connectivity network of EU countries introduces risks of sabotage and spying, possibly compromising these networks.

On the other hand, LEO services offer opportunities to strengthen the EU's strategic autonomy. LEO constellations can complement cable-based internet by providing a contingency in case of damage to ground communications and have greater resilience against attacks due to their large numbers of satellites. This capability is strategically relevant to the EU as the bloc relies on undersea internet cables exposed to damage and sabotage. Lastly, an LEO constellation could amplify EU military capabilities by enabling high-speed military communications and data transfer, and global remote sensing. These capabilities are important in the current context of autonomous and AI-enabled warfare. Against this backdrop, it remains to be seen whether the EU will succeed in developing its space industry and launching IRIS², and whether the latter will deliver sufficient capabilities.

Because of the tremendous increase of satellites launched in orbit, proliferated LEO constellations are also sparking increasing concerns about risks of collisions, space debris, and interference with astronomical observations. Although such issues fall outside the scope of this article, it is important to consider the spillover impacts on space security that LEO constellations may cause and the need for new international regulations to ensure the long-term sustainability of space activities.

References

Abels, J. (2024). Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine. *European Journal of International Relations, 0*(0), 1-25. https://doi-org.ezproxy.leidenuniv.nl/10.1177/13540661241260653

Alvarez, S. (2023, August 31). Starlink a key technology for Brazil's military: Department of Ministry letter. *TESLARATI*. https://www.teslarati.com/starlink-key-technology-brazil-military-department-of-ministry-letter/

Alvarez, S. (2024, May 21). Starlink celebrates new milestone: 3 million customers in 99 countries. *TESLARATI*. https://www.teslarati.com/starlink-celebrates-3-million-customers-99-countries/

Kaushik, R. & Selvamurthy, W. (2023). Starlink's role in Ukraine: Portent of a space war? *Manohar Parrikar Institute for Defence Studies and Analyses Journal of Defence Studies, 17*(1), 25–44. https://www.idsa.in/jds/17-1-2023-Starlink-Role-in-Ukraine

Bergengruen, V. (2022, October 18). The battle for control over Ukraine's internet. *TIME*. https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/

Boley, A., & Byers, M. (2024). Anti-satellite weapon tests to disrupt large satellite constellations. *Nature Astronomy, 8*, 10–12. https://doi.org/10.1038/s41550-023-02173-9

Brito, R., & Magalhaes, L. N. (2024, September 3). Starlink emerges as fresh battleground between Musk, Brazil. *Reuters*. https://www.reuters.com/technology/brazils-supreme-court-chamber-forms-majority-uphold-x-suspension-2024-09-02/

Congressional Budget Office (CBO). (2023). *Large Constellations of Low-Altitude Satellites: A Primer*. https://www.cbo.gov/publication/58794

Council on Foreign Relations. (n.d.). *Assessing China's Digital Silk Road Initiative.* https://www.cfr.org/china-digital-silk-road/

Council of the European Union. (n.d.). *EU space policy*. Retrieved September 8, 2024, from https://www.consilium.europa.eu/en/policies/eu-space-programme/#why

Cellerino, C. (2023). EU space policy and strategic autonomy: Tackling legal complexities in the enhancement of the 'security and defence dimension of the Union in space'. *European Papers, 8*(2), 487-501. https://doi.org/10.15166/2499-8249/669

Cerulus, L. (2020, May 26). Trump and friends: Where European countries come down on Huawei. *Politico*. https://www.politico.com/news/2020/05/26/europe-huawei-5g-281701

Daehnick, C., Hamill, R., Ménard, A., & Wiseman, B. (2022, August 11). Is there a 'best' owner of satellite internet? *McKinsey & Company*. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/is-there-a-best-owner-of-satellite-internet

Damen, M. (2022). *EU strategic autonomy 2013-2023: From concept to capacity*. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589

Davis, M. (2022). The implications of commercial space: From enabling military capability to introducing new dynamics into competition. *The Air Power Journal.* https://theairpowerjournal.com/the-implications-of-commercial-space-from-enabling-military-capability-to-introducing-new-dynamics-into-competition/

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2023, March 10). *European Union Space Strategy for Security and Defence* (JOIN(2023) 9 final). https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en

European Commission. (n.d.). *EU space strategy for security and defence*. Retrieved September 8, 2024, from https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

European Commission. (n.d.). *IRIS²: The new EU secure satellite constellation: Infrastructure for resilience, interconnectivity and security by satellite*. Retrieved September 8, 2024, from https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

European Defence Agency (EDA). (n.d.). *"Ukraine war confirms need to define a long-term strategy to ensure the defence of Europe."* Retrieved September 20, 2024, from https://eda.europa.eu/webzine/issue23/interview/ukraine-war-confirms-need-define-long-term-strategy

European Space Policy Institute (ESPI). (2022). *IRIS2: The new (material) girl on the block* (Brief No. 61). https://www.espi.or.at/briefs/iris2-the-new-material-girl-on-the-block/

European Union Agency for the Space Programme (EUSPA). (2024, April 26). *IRIS².* Retrieved from https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2

Evroux, C., Heflich, A., & Saulnier, J. L. (2023). *Towards EU leadership in the space sector through open strategic autonomy: Cost of non-Europe* (PE 734.691). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/734691/EPRS_STU(2023)734691_EN.pdf

Froehlich, A. (Ed.). (2021). *Legal aspects around satellite constellations: Volume 2*. Cham, Switzerland: Springer. http://dx.doi.org/10.1007/978-3-030-71385-0

Giles, K. (2023). Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine. *Chatham House,* 0-61. https://doi.org/10.55317/9781784135898.

Hallex, M. A., & Cottom, T. S. (2020). Proliferated commercial satellite constellations: Implications for national security. *Joint Force Quarterly, 97*, 20-29. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106495/proliferated-commercial-satellite-constellations-implications-for-national-secu/

Harrison, T. (2024). *Building an enduring advantage in the third space age*. American Enterprise Institute. https://www.aei.org/research-products/report/building-an-enduring-advantage-in-the-third-space-age/

Harrison, T., & Strohmeyer, M. (2022). *Commercial space remote sensing and its role in national security*. Center for Strategic and International Studies. https://www.csis.org/analysis/commercial-space-remote-sensing-and-its-role-national-security

Helwig, N., & Sinkkonen, V. (2022). Strategic autonomy and the EU as a global actor: The evolution, debate and theory of a contested term. *European Foreign Affairs Review, 27* (Special Issue), 1–20. https://doi.org/10.54648/EERR2022009

International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. ITU Publications. https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/.

Jayanti, A. (2023, March 9). Starlink and the Russia-Ukraine War: A case of commercial technology and public purpose? *Belfer Center for Science and International Affairs*.

https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Jones, A. (2022, February 17). Shanghai signs agreement with China's megaconstellation group, aims to foster commercial space hub. *Space News*. https://spacenews.com/shanghai-signs-agreement-with-chinas-megaconstellation-group-aims-to-foster-commercial-space-hub/

Jones, A. (2024, April 19). China to leverage growing commercial space sector to launch megaconstellations. *Space News*. https://spacenews.com/china-to-leverage-growing-commercial-space-sector-to-launch-megaconstellations/#:~:text=Nebula%2D1%20rocket.-,Company,-Rocket%20Name

Jones, A. (2024, August 6). China launches first satellites for Thousand Sails megaconstellation. *Space News*. https://spacenews.com/china-launches-first-satellites-for-thousand-sails-megaconstellation/

Khalaf, R. (2022, October 7). Elon Musk: 'Aren't you entertained?' *Financial Times*. https://www.ft.com/content/5ef14997-982e-4f03-8548-b5d67202623a

Kuhr, J. (2024, January 4). 2023 orbital launches, by country. *Payload*. https://payloadspace.com/2023-orbital-launches-by-country/

Küsters, A., Nolen, N., & Stockebrandt, P. (2024, February 20). Strategic autonomy in EU space policy: Securing Europe's final frontier through launches, laws, and space mining. *Center for European Policy cepInput, 4*, 1-25. https://www.cep.eu/eu-topics/details/strategic-autonomy-in-eu-space-policy-cepinput.html

Osisanya, S. (n.d.). *National security versus global security.* UN Chronicle. Retrieved September 8, 2024, from https://www.un.org/en/chronicle/article/national-security-versus-global-security.

Page, M. (2023, October 31). Russia, a Chinese cargo ship and the sabotage of subsea cables in the Baltic Sea. *The Strategist*. https://www.aspistrategist.org.au/russia-a-chinese-cargo-ship-and-the-sabotage-of-subsea-cables-in-the-baltic-sea/

Page, M. (2024, August 26). China may be putting the Great Firewall into orbit. *The Strategist*. https://www.aspistrategist.org.au/china-may-be-putting-the-great-firewall-into-orbit/

Paraguassu, L., Benedito, L. M., & Brito, R. (2024, August 31). Brazil watchdog moves to block access to Elon Musk's X after court order. *Reuters*.

https://www.reuters.com/technology/lula-says-musk-must-respect-brazils-top-court-x-braces-shutdown-2024-08-30/?taid=66d20650d8471d00018ff127&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter.

Pelton, J. N., & Madry, S. (Eds.). (2020). *Handbook of small satellites: Technology, design, manufacture, applications, economics and regulation*. Cham, Switzerland: Springer.

Phillips, T., & Milmo, D. (2024, September 8). 'Can't live without it': Alarm at Musk's Starlink dominance in Brazil's Amazon. *The Guardian*. https://www.theguardian.com/technology/article/2024/sep/08/alarm-at-musk-starlink-dominance-brazil-amazon

Pultarova, T., Howell, E., Mann, A., & Dobrijevic, D. (2024, August 29). Starlink satellites: Facts, tracking and impact on astronomy. *Space.com.* https://www.space.com/spacex-starlink-satellites.html.

Radhakrishnan, R., Edmonson, W. W., Afghah, F., Martinez Rodriguez-Osorio, R., Pinto, F., & Burleigh, S. C. (2016). Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. *IEEE Communications Surveys and Tutorials, 18*(4), 2442–2473. https://doi.org/10.1109/COMST.2016.2564990

Reuters. (2024, February 15). Russia using thousands of SpaceX Starlink terminals in Ukraine, WSJ says. *Reuters*. https://www.reuters.com/world/europe/russia-using-thousands-spacex-starlink-terminals-ukraine-wsj-says-2024-02-15/

Reuters. (2023, September 29). European countries who put curbs on Huawei 5G equipment. *Reuters*. https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/

Roulette, J., & Taylor, M. (2024, March 16). Exclusive: Musk's SpaceX is building spy satellite network for US intelligence agency, sources say. *Reuters*. https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/

Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. *Center for Strategic and International Studies.* https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Satariano, A., Reinhard, S., Metz, C., Frenkel, S., & Khurana, M. (2023, July 28). Elon Musk's unmatched power in the stars. *The New York Times.* https://www.nytimes.com/interactive/2023/07/28/business/starlink.html

Schrogl, K.-U. (Ed.). (2020). *Handbook of space security: Policies, applications and programs* (2nd ed.). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-23210-8

SES. (2023, April 11). *Building a secure resilient satellite infrastructure for Europe*. https://www.ses.com/newsroom/building-secure-resilient-satellite-infrastructure-europe

SpaceX. (n.d.). *Starlink*. Retrieved September 29, 2024, from https://www.starlink.com/

SpaceX. (n.d.). *Starshield: Supporting national security*. Retrieved September 30, 2024, from https://www.spacex.com/starshield/

Starlink. (n.d.). *Satellite technology*. Retrieved September 8, 2024, from https://www.starlink.com/technology

Starlink. (n.d.). *Starlink coverage map*. Retrieved September 20, 2024, from https://www.starlink.com/map

Suess, J. (2023, May 3). Commentary: Guo Wang: China's answer to Starlink? *The Royal United Services Institute (RUSI)*. https://rusi.org/explore-our-research/publications/commentary/guo-wang-chinas-answer-starlink

United Nations. (2023, October 19). *Outer space becoming contested domain for supremacy with space-based communications, intelligence assets, anti-satellite weapons, First Committee hears*. United Nations Press. https://press.un.org/en/2023/gadis3722.doc.htm

Voelsen, D. (2021). Internet from space: How new satellite connections could affect global internet governance. *Stiftung Wissenschaft und Politik Research Paper 03*, 0-31. https://doi.org/10.18449/2021RP03

Wall, C., & Morcos, P. (2021, June 11). Invisible and vital: Undersea cables and transatlantic security. *Center for Strategic and International Studies (CSIS)*. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Wiedemar, S. (2023). Nouvelles frontières de la militarisation de l'espace. *CSS Analyses in Security Policy, 333*, 1-4. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse333-FR.pdf

Young, M., & Thadani, A. (2022). *Low orbit, high stakes: All-in on the LEO broadband competition*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/low-orbit-high-stakes

Zhang, J., Cai, Y., Xue, C., Xue, Z., & Cai, H. (2022). LEO mega constellations: Review of development, impact, surveillance, and governance. *Space: Science & Technology, 2022*, 1-17. https://doi.org/10.34133/2022/9865174