

The Politics of Dual-Use Technology: Starlink and the War in Ukraine

Ravale Mohydin



(Metin Aktaş - Anadolu Agency)

Technology politicisation is a complex and multifaceted phenomenon. It can occur at various stages of technological development and deployment. Starlink, a satellite internet service offered by SpaceX, exemplifies this issue. The firm aims to deliver global internet coverage, which is quintessential for rural and geographically remote areas. However, it has raised concerns due to its dual-use nature and potential role in the ongoing dispute with Russia. This policy outlook will examine this predicament, focusing on Starlink's significance not just for the Ukraine conflict but also for the dual-use technologies' utilisation in international security.

Introduction

The rise of dual-use technology, which has both civilian and military applications, has become a source of geopolitical tension in recent years. This situation is particularly true for Starlink, a satellite internet service offered by SpaceX, which has the potential to provide internet access to remote and underdeveloped regions around the world. However, using Starlink in Ukraine has raised concerns about the politicisation of dual-use technology and its potential role in the ongoing conflict with Russia. This policy outlook will examine the politicisation of dual-use technology in the context of the war in Ukraine, specifically focusing on the use of Starlink and its implications not just for the conflict but also the continued support for dual-use technologies, highlighting the near-sightedness of relying on public-private partnerships for international security.

Politicisation of Technology

Technology politicisation is a complex and multifaceted phenomenon. It can occur at various stages of technological development and deployment. At its core, it involves the interaction between technology and politics, which can take many forms. For example, technology can be used for political advocacy, such as when social media platforms are used to [mobilise political campaigns or protests](#). Conversely, political actors [may seek to influence](#) the development and deployment of technology to achieve political goals, such as by investing in research and development of specific technologies or regulating the use of certain technologies in particular contexts. Technology politicisation can also involve debates over technology's [social and ethical implications](#), such as the impact of automation on employment or the ethical considerations of using artificial intelligence in decision-making processes. Political values and ideologies, such as concerns over privacy, data ownership, and individual rights, may shape these debates. In some cases, the politicisation of technology can lead to conflict, as different political actors or interest groups may have competing visions for the role of technology in society. For example, using technologies like drones or surveillance systems may threaten [the civil liberties](#) of some groups, while others may see them as essential tools for national security.

Then there are types of technologies and innovations that are less defined in terms of use or cannot be limited to one use or another. There are [different perspectives on technology](#), with some viewing it as a product or artefact and others as a system of social relations. The dual-use concept is situated at the intersection of these two views of technology. [Dual-use technologies](#) have the potential for both civilian and military or security applications. They can be developed for peaceful purposes but also have the potential to be adapted or modified for military or security-related uses.

The development and implementation of such technologies carry an inherent risk for politicisation.

The Growing Importance of Technology in Warfare

The importance of technology in warfare increased significantly in the 19th century due to the Industrial Revolution, state sponsorship of technological innovation, and the state's role in maintaining the credibility of nuclear deterrence. The state's investment in defence research facilitated a [profound change in the relationship between the state and private industry](#), creating a military-industrial complex. However, the end of the Cold War resulted in a significant reduction in defence expenditure and a shift towards private sector involvement in defence production. Most western governments promoted the exploitation of technologies created through government-funded defence research as a means of [generating wealth creation](#). The civil and commercial sectors proved adept at adapting and changing new capabilities, leading to an increasing emphasis on the existing pool of tech savviness within the broader economy. The trend towards greater complexity during operations facilitated the rise of private military companies in the post-Cold War era, resulting in western states increasingly subcontracting internal and external security to the private sector.

In 1995, US President Bill Clinton's administration introduced a [new dual-use technology policy](#) that changed the traditional approach of the US Defense Department (DoD) towards technology development. Under this policy, the DoD had commercial considerations and adopted more flexible contractual arrangements, such as partnerships, with the commercial industry. Besides the fact that Western governments were now more likely to exploit created through government-funded defence research for wealth creation, as noted above, this shift was also necessary because the DoD [could no longer afford](#) the long acquisition cycle times it historically had. The DoD's dual-use investment strategy (documented in a [report](#) entitled Dual-Use Technology: A Defense Strategy for Affordable, Leading-Edge Technology) had three pillars: leveraging the commercial sector's technology-based investment, emphasising ["dual produce"](#) to take advantage of commercial production for subsystems or critical components, and investing in the necessary technologies to facilitate the use of commercial components in defence systems. The objective was to shorten acquisition cycle times and apply commercial technologies to meet the DoD's mission needs.

The concept of dual-use technology is [complex and dynamic](#). It refers to the potential for a technology to have

both civilian and military applications. It is important to note, though, a dual-use technology product's potential may not always be realised, as the duality of technology is "[dependent on the social network](#)" in which it is developed and used or may become apparent later in its development. This means that any technology's civil, military, or dual-use aspects may shift and change over time as the technology develops and the actors involved change.

The US government has implemented various dual-use investment strategies to enhance military reliance on the industrial base of the commercial sector. These include purposeful and serendipitous spin-offs, direct and indirect spin-on, and industrial base-strengthening [strategies](#). Purposeful spin-off involves consciously funding activities that seek commercial applications for defence capabilities, while serendipitous spin-off refers to funding activities that coincidentally lead to the commercialisation of defence capabilities. Direct and indirect spin-on strategies have been employed in response to declining defence budgets and rapid advancements in commercial technologies. Direct spin-on involves funding the acquisition of commercial off-the-shelf products, processes, or technologies that require minimal modification for military use.

In contrast, indirect spin-on entails funding activities in the commercial sector to influence their development into capabilities that meet the needs of both the military and commercial sectors. Additionally, an industrial base strengthening strategy has been observed in the literature. This approach aims to address the broader role of the commercial sector in national security, as well as creating jobs for US citizens, promoting domestic production activities, and improving the balance of payments. This strategy also aims to improve opportunities for the military to leverage commercial capabilities.

However, there are challenges for dual-use technologies, including the differences between the commercial and military sectors and the practical limits of dual-use. While some military requirements can be met by commercial industry, others cannot be due to their specific needs and practices. Even with great effort, some military technologies are just not compatible with commercial needs. Despite these challenges, there have been successful examples of military technologies being spun off to the commercial sector, such as "the [development](#) of microelectronics, supercomputers, commercial jet aircraft and aircraft engines, the global positioning system, and composite materials".

SpaceX, the technology company owned by billionaire Elon Musk (the CEO), has also received US government funding from various sources, including the Department of Defense (DoD) and NASA. Starlink is a [satellite internet constellation](#) developed by SpaceX. The constellation consists of thousands of small satellites that orbit the Earth at low altitudes, providing high-speed internet access to re-

mote and underserved areas around the world faster and more reliably. In addition to its potential for improving global communication and connectivity globally, Starlink could also support the development of autonomous vehicles and smart cities by providing a reliable and fast internet connection to support their operation.

On the one hand, investment by the US government in SpaceX can be said to be intended to support the [development of a private space industry](#), which aligns with the goals of the commercial industry. By investing in SpaceX, the US government may intend to support the development of new technologies and capabilities that the private sector can leverage to create economic value and drive innovation. Even though SpaceX is a private company, its mission is to reduce the cost of space travel and exploration, which can help create new markets and opportunities for commercial space activities. This is also in the US government's interest in terms of domestic job creation and international competition and maintaining the edge in space exploration. From the perspective of wealth generation, it makes sense for the US government to invest in SpaceX.

Thus, SpaceX has received [significant funding](#) from the National Aeronautics and Space Administration (NASA) for space transportation services. These contracts include the Commercial Resupply Services (CRS) program, which involves delivering cargo to the International Space Station (ISS), and the Commercial Crew Program (CCP), which involves developing a spacecraft capable of transporting astronauts to and from the ISS. SpaceX has also received funding from NASA for developing the Starship spacecraft, intended for future missions to the Moon and Mars. SpaceX's Starlink also [received 886 million USD](#) from the US government to fund high-speed internet projects in underserved areas across 35 states. Another potential application of Starlink is in earth observation and climate monitoring. Many experts believe the investment in SpaceX will return handsome profits now and in the future.

Yet, the investment in SpaceX also has a military aspect. With funding secured from the [Pentagon](#), SpaceX is developing advanced rocket technologies and launch capabilities with direct applications in the defence sector. For example, the Falcon 9 rocket, developed by SpaceX, has been used by the US government to launch satellites for military and intelligence purposes. The [Dragon spacecraft](#), also developed by SpaceX, has the potential to be used for military logistics and transport missions. SpaceX has also received funding from other government agencies, such as the National Reconnaissance Office (NRO), responsible for developing and operating reconnaissance satellites for the US.

Against the backdrop of the Russian invasion of Ukraine in 2022, it was reported that the US Agency for International Development (USAID) had also "delivered 5,000 Starlink Terminals to the Government of Ukraine [through](#)

[a public-private partnership](#) with the American aerospace manufacturer, SpaceX, a private sector donation valued at roughly 10 million USD" with SpaceX donating "3,667 terminals and the internet service itself, and [USAID purchased](#) the additional 1,333 terminals" in April 2022. USAID spent roughly 3 million USD on hardware and services in the country. With that said, Pentagon Press Secretary General Pat Ryder stated that the ["DoD has not paid SpaceX any money](#) for Starlink services in Ukraine" in October 2022. It can be deduced from the careful navigation on display by US authorities regarding the source of funding for SpaceX's Starlink in Ukraine that significant risks are involved in balancing priorities on international relations, national security as well as global security while using dual-use technologies.

Starlink and the Russian-Ukrainian Conflict

Before getting into the role played by Starlink in the Russian invasion of Ukraine, providing background information may be useful. The conflict between Ukraine and Russia has its roots in the [country's complicated history and geopolitical position](#). Ukraine has long been a crossroads between Eastern and Western Europe, and its people and culture have been influenced by both. After the collapse of the Soviet Union in 1991, Ukraine gained independence and established its government and economy.

However, Ukraine's relationship with Russia remained complex, with many Ukrainians identifying as both Ukrainian and Russian and deep economic and cultural ties existed between the two countries. In 2013, President Yanukovich [rejected a trade agreement with the European Union \(EU\)](#) in favour of closer ties with Russia, sparking protests and unrest across the country. Yanukovich was eventually removed from power in February 2014, and Russia responded by annexing Crimea, a peninsula on the Black Sea with a large Russian-speaking population.

The international community widely condemned this move, and the conflict quickly escalated into a military conflict in eastern Ukraine between Ukrainian government forces and Russian-backed separatists. The separatists declared independence and established [self-proclaimed republics](#) in the Donetsk and Luhansk regions, which Ukraine and the international community did not recognise.

Since then, the conflict has had a devastating impact on Ukraine, with [thousands of people killed and millions displaced](#). The Ukrainian economy has also been severely affected, with the conflict disrupting trade and causing significant damage to infrastructure. The conflict has also caused tensions between Russia and Western countries,

with the US and the EU imposing economic sanctions on Russia. Attempts to resolve the conflict have been made through diplomatic means, including signing agreements such as the [Minsk Protocol](#) and the Minsk II agreement. However, these accords were not implemented, and the conflict continues today. The situation remains complex and ongoing, with no clear resolution in sight.

In the ongoing conflict between Russia and Ukraine, the US company SpaceX's Starlink service has played a [crucial role](#) in keeping Ukraine's military and citizens online as Russia targets Ukraine's telecommunications and electricity infrastructure. Starlink's lower-orbiting satellites have enabled troops to communicate with each other on the battlefield, NGOs to operate effectively, and even enabled drones and weapons systems to stay operational. As per CNN, it is hard to ["overstate"](#) the impact Starlink has had on the war in Ukraine. Reports in October 2022, however, indicated that there were widespread Starlink outages in Ukraine, particularly as Ukrainian troops attempted to regain control of territories in the eastern and southern parts of the country from Russian occupation. According to sources familiar with the situation, the outages suddenly affected the entire frontline on September 30, impacting the Ukrainian army's ability to communicate effectively. As a result, units on the battlefield have since had to rely on other means of communication, causing a ["catastrophic"](#) loss of communication, as per the Financial Times.

The outages caused concern in Ukraine about [Musk's allegiance](#). This concern was further exacerbated by Musk's recent tweet about a [peace plan](#) that would have Ukraine surrender Crimea and control over the eastern Luhansk and Donetsk regions (despite this, Musk has affirmed his support for Ukraine and denied speaking to Putin directly about the situation). Then, SpaceX requested that the [US military pay for the ongoing costs](#) of providing Starlink internet service to Ukraine. According to SpaceX, about 85 per cent of the 20,000 Starlink terminals in Ukraine were paid for by countries like the US and Poland or other entities, paying for about 30 per cent of the internet connectivity. SpaceX claims that the ongoing costs have gotten too high and are approaching 100 million USD, leading the company to ask the DoD to pick up Ukraine's new request for 6,200 more terminals and ongoing service costs, which could total almost 380 million USD for one year.

As a result, Ukraine's use of SpaceX's Starlink internet service during the ongoing conflict with Russia has become a contentious issue, with SpaceX President Gwynne Shotwell stating that the company did not intend for Starlink to be ["weaponised"](#). Shotwell clarified that while military use of Starlink is acceptable, using it for offensive purposes was never intended, and she expressed concerns about Ukraine using it on drones. SpaceX did not provide details on limitations but referred to the Starlink terms of service, prohibiting its use for offensive or defensive weaponry. Following that, former NASA astronaut Scott Kelly called on

Musk to restore full functionality to Starlink via a Twitter exchange, and while Musk emphasised that Starlink is crucial for Ukraine's communication, SpaceX will not enable the escalation of conflict. Specifically, Musk tweeted that "Starlink is the [communication backbone](#) of Ukraine...[but Starlink] will not enable escalation of conflict that may lead to WW3". In a separate tweet, Musk said, "we have not [exercised our right](#) to turn them off".

The Politics of Dual-Use Technologies

Given the backdrop, the decision to keep Starlink running or not lies solely in the hands of Musk, the CEO of SpaceX. This has raised concerns about the extent of his power in the matter and the potential risks associated with having such a critical infrastructure controlled by a single individual. If Musk decides so, Ukraine [may be at risk of a sudden cutoff](#) of service. For all countries that become increasingly dependent on critical infrastructure developed by private companies, a sudden loss of internet access could have severe consequences for their ability to communicate and coordinate effectively in the event of a war or political crisis. It must be noted that it would be a perfectly legal move for the private company. Moreover, in economic terms, the [risks of monopolistic control](#) over any product, in general, may mean it would be difficult for other companies to enter the market and compete, potentially leading to higher prices and reduced quality of service. In particular, the risks of monopolistic control over critical infrastructure may translate into extortionary prices and unreliable supply, which can be disastrous in critical times.

[Research](#) distinguishes between spillover and duality in technology. Spillover refers to a situation in which research is conducted in one domain and then [adopted without change in another domain](#). This is not evidence of duality but rather the absence of it. The potential for duality is dependent on the networks of the technology. This raises the issue of dual-use technology transfer, when a technology originally designed for military or civilian use is transferred to the opposite application, potentially requiring a change in its intended purpose. Duality in technology is closely linked to dual-use technology transfers, which occur when there is an explicit intention to modify a technology's original military or civilian application. As a private company, Starlink has the autonomy to determine its terms of use. While the primary application of the technology is for communication purposes, there have been indications that it could have dual-use potential, including for the interception of drones. This would represent a change in the initial purpose of the technology. The extent to which Starlink intends to pursue such applications, if at all, has not been made clear.

However, about Ukraine, SpaceX President Gwynne Shotwell stated that the [technology was not intended to be weaponised](#) in February 2023. Shotwell acknowledged that Ukraine had used Starlink in ways that were unintentional and not part of any agreement. She further indicated that while using Starlink as a communication system for the military was acceptable, the company never intended for the technology to be used for offensive purposes, such as connecting drones to identify and destroy enemy targets. When asked about the potential limitations that SpaceX could impose to prevent Ukraine from using Starlink in such a manner, Shotwell did not provide specific details but noted that there were measures that could be taken to limit such use. Even though SpaceX has not disclosed what these limitations are or whether they are still in effect, the company's Starlink terms of service agreement for the US prohibits the modification of SpaceX equipment or service that would violate US export laws and specifies that Starlink is not designed or intended for use with offensive or defensive weaponry or similar end-uses.

The fact that Starlink's operations in Ukraine have been partially funded by the US, United Kingdom (UK), and Poland adds more complexity to the situation. Firstly, it highlights the level of involvement of these governments in the provision of critical infrastructure during times of war. This could be seen as a departure from [traditional approaches to foreign aid](#), which have typically focused on providing military and humanitarian assistance (the military assistance is typically in the form of simplifying mechanisms for procuring weapons or security contracts) rather than directly funding infrastructure projects. Military assistance to Ukraine in the form of building defence infrastructure could have significant implications for the ongoing conflict with Russia. While it may signal support from the West and deter further aggression from Russia, it also has the potential to [escalate the conflict](#) and increase the risk of a larger conflict. Secondly, the involvement of these governments in funding Starlink's operations in Ukraine underscores the potential for geopolitical influence and control over critical infrastructure. This could be seen as a form of [soft power](#), where governments use their economic and technological resources to [exert influence](#) and shape the behaviour of other countries. Finally, the involvement of these governments in funding Starlink's operations in Ukraine highlights the complex and interdependent nature of modern warfare. As conflicts become increasingly reliant on technology, the provision of critical infrastructure can have significant strategic implications and be used as a tool for offence and defence.

Maintaining Starlink connectivity at a nominal cost to Ukraine's military is critical to avoid [putting Ukrainian soldiers in direct danger](#). Therefore, finding a mutually agreeable solution that ensures the continued provision of this essential service in the near term is necessary. While SpaceX cannot be held solely accountable for the associated costs, avoiding adopting a victim mentality is

important. SpaceX entered this venture with full knowledge of the potential expenses involved but apparently without a clear plan for covering these costs. Likewise, the Ukrainian (or any) government cannot reasonably expect SpaceX to bear the entire financial burden of the hardware and software expenses. However, both parties must establish a clear agreement regarding appropriate use, cost sharing and financial responsibility from the outset. Given that, all parties involved, including SpaceX, the American, British, Polish, and Ukrainian governments, as well as the Ukrainian military, should exercise responsible use of Starlink technology to further avoid conflict escalation. This includes adhering to established guidelines, avoiding any illegal or unethical activities, and promoting the peaceful and constructive use of the technology.

With that said, bigger questions are at play regarding the longer-term strategy for dual-use technologies. The lack of a comparable service offered by Western, particularly the US, governments in Ukraine, irrespective of the significant military and humanitarian aid they have provided, has raised concerns. Governments and international organisations are responsible for ensuring that critical infrastructure provision during times of war is transparent, accountable, and in the best interest of all parties involved. This includes ensuring that the provision of critical infrastructure does not compromise national security or sovereignty and that mechanisms are in place to ensure such systems' long-term sustainability and reliability. Private companies, such as SpaceX, may not be the most sustainable solution not only because of their ability to operate independently and impartially due to potentially being subject to political pressure or influence from their funders but also because accountability and transparency may become issues. Unlike government agencies, private companies are not subject to the same level of public scrutiny and oversight, which could make it more difficult to assess their actions and intentions, potentially making it a national security concern. Objectively speaking, the security of such a strategy is compromised. The politics of dual-use technology, such as Starlink in the Russian-Ukrainian conflict, have only highlighted the near-sightedness of relying on public-private partnerships for global security, particularly given the privileges afforded to private enterprise in the neoliberal financial system.