Luiss
School of Government

An overview of space and digital integration

Working Paper Series
SOG-WP10/2024

Author: Wagner Benoit
May 2024

LUISS

Table of Contents

1. Abstract

This article attempts to provide a general overview of the transformations taking place within the space sector under the influence of digital technology. These changes are as much related to the emergence of digital players within the important space sector, with their logic and practices, as they are to technological transformations. This evolution of the space sector also has consequences for the security of space activities and for the balance of power between states.

Keywords: space, digital, New space, international relations

2. Introduction

"Space is the cornerstone of today's society"[1], a phrase which, in itself, is sufficient to highlight the stakes involved in mastering the space environment. Space can be seen as a strategic resource, underpinning the development of a large number of sectors of our society, including telecommunications, the media, the economy, agriculture, the environment and national defence.

The history of space began during the Second World War with the development of the V2 missile by the Third Reich, in order to bomb England. But the use of space really took off during the Cold War, on the one hand, to justify the superiority of one ideological and political model over the other (communism and capitalism), and on the other hand, because the conquest of space held a certain prestige. After the successful launch of Sputnik 1 in 1957 and Yuri Gagarin's achievement in 1961, the Americans in turn felt obliged to accomplish a technical feat in order to further consolidate their ideological model. Indeed, JFK had no real interest in the Moon when he launched the Apollo program; his only desire was to demonstrate a master stroke even more impressive than a man's journey into space.

On the other hand, the development of the space sector is closely linked to the emergence of nuclear strategy, and therefore to strategic issues. For the USSR, it was a question of being able to strike a distant territory, which led them to develop the intercontinental missile. For the Americans, it was more a question of being able to acquire and exploit data concerning the enemy's nuclear positions and weapons. The space sector has therefore rapidly become a major strategic issue and has developed further in recent years, with systems destined to be increasingly integrated into the military apparatus as well as into economic life.

In the military sphere, space-based resources are used to support operations both with observation capabilities and with telecommunications capabilities to set up certain tactical data links and listening capabilities. This is also, through the PNT function[2] which can be found in navigation systems and in new combat and command information systems such as the Scorpion platform[3] which require very fine synchronization capabilities. Space technologies are also used for early warning[4] and ballistic missile defence, i.e., the monitoring of ballistic missile launches and testing activities, which is an essential component of nuclear deterrence.

In the civil sector, there is also an earth observation function for mapping, producing meteorological data and analyzing natural, climatic and environmental risks. A telecom function (Internet, telephony, satellite

[1] Jean-Pierre Serra, VP airbus defense and space, symposium on spacecraft surveillance and security, December 4, 2017
[2] Positioning, Navigation and Timing, GNSS (Global navigation satellite system) function
[3] The SCORPION (synergie du contact renforcée par la polyvalence et l'infovalorisation) system is a combat and command system for the French army, launched in 2018, which aims to align the capabilities of joint battle groups by federating platforms and combatants around a single information and communication system.
[4] Although after the success of the SPIRALE demonstrator in 2014, the development of the program has fallen behind schedule.

TV) and the global navigation space system (GNSS)/PNT function, for geo-navigation and synchronization of various networks such as digital, banking, financial and energy distribution networks. Satellites are also used for scientific missions. The space sector thus appears to be the privileged domain of the state, with its economic, military and political sovereignty at stake. However, the 2000s saw the emergence (in Silicon Valley) of a phenomenon known as "New Space", which can be defined as the rapid growth of private players linked to the digital world, in a context of liberalization of the space sector.

Similarly, the space sector has an increasingly close relationship with cyberspace[5], as it helps to expand and develop it, not only by producing data through various space-based capabilities (such as PNT systems, which help to synchronise information systems) but also by creating new connections through telecommunication satellite resources.

Twenty years after the emergence of the New Space movement, we can observe a strong revival of the militarization of space and the emergence of new economic rivalries.[6] In line with this logic, space technologies seem to be becoming increasingly digitized and marked by the practices of the digital world. This raises the question of whether we are indeed witnessing a digital transformation of the space sector, and what consequences this might have in the current geopolitical context.

First, we will look at the gradual transformation of the space sector, and how the players and their practices are transforming it. Secondly, we will look at the consequences of these transformations, in terms of both the security of space activities and their impact on existing international rivalries.

[5] For the Agence nationale de sécurité des systèmes d'information, cyberspace is understood as a "communication space constituted by the worldwide interconnection of automated digital data processing equipment". https://www.ssi.gouv.fr/particulier/glossaire/c/.

[6] The last two years have seen, among other things, the creation of the Space Force in the United States, a new command dedicated to space activities in France, and an Indian space and defense agency. India's6 ASAT launch test in March 2019 is also noteworthy, despite the fact that this country has always positioned itself as a peaceful space power, prioritising civilian rather than military programs. We should also mention Russia's ASAT tests in 2020.

3. The transformation of the space sector is increasingly influenced by digital players and their practices.

One of the first aspects of the rapprochement that can be observed between the space and digital sectors is the emergence of digital players who bring with them their ideology based on a borderless, hyper-globalized society, which, as Monique Dagnaud points out, can be found in part in the Californian model, and which is expressed in part by the concepts of "free of charge" and "free speech".[7]

The "free of charge" concept is reflected in the idea that New Space aims to disrupt the market, as demonstrated once again by the example of SpaceX, which aims to reduce launch costs by creating reusable launchers, with the aim of halving prices. As a consequence, a Falcon 9 launch should cost around 60-70 million dollars, compared with 120 million for Ariane 5.[8]

In addition, since the late 2000s there has been a strong involvement of GAFAMs (Google, Apple, Facebook, Amazon) in New Space, the prime example being the recent partnership between SpaceX and Microsoft (Azure)[9] as SpaceX COO Gwynne Shotwell points out: "This collaboration will enable us to work hand-in-hand with Microsoft to bring new offerings to the public and private sectors to provide connectivity through Starlink for use on Azure. Where this makes sense is that we plan to work with Microsoft to leverage our mutual customers and discover new sets."[10] The use of outer space enables facilities in terms of data collection and sharing capacity, which translates into a considerable extension of cyberspace.

As Xavier Pasco points out, space technologies are necessary for the digital giants to expand their activities by providing more widespread high-speed Internet access, and the applications that go with it.[11] This is made possible by super-constellations and even mega-constellations of satellites (more than a thousand), which imply new production models for space technologies that were previously based on cutting-edge technology. Indeed, to ensure the smooth operation of these constellations, new production models are needed, requiring maximum reproducibility with the same level of quality and reliability.

These new technologies are of particular interest to the digital giants, as they will enable them to expand the market in which they already operate. They will enable them to spread the possibilities of high-speed Internet access more widely, as well as the resulting applications, as Eutelsat is already doing. Besides, as Internet technology is extremely fast-moving, its players need maximum responsiveness to ensure their

[7] Monique Dagnaud, Olivier Alexandre, seminar on the Californian model, November 21, 2017
[8] Even if Falcon 9 launchers don't offer the same reliability as Ariane 5, this remains an important issue for the delivery of certain payloads, which can be very costly to manufacture.
[9] Xavier Pasco, « New forms of competition in space ». Revue Défense Nationale, 2022.
[10] Valentin Cimino, Microsoft and SpaceX team up to connect the Starlink satellite network through the cloud, digital century, 2021
[11] Xavier Pasco, The New Space Age. From the Cold War to the New Space, CNRS éditions, 2017

business model; as was the case with SpaceX during the war in Ukraine. Here we find the idea of the hyper-globalized society, which is obviously in the ideological model of digital players.

Along the same line, it is worth noting that the digital players have also imported their practices and business models into the space sector. We can therefore observe three specific business models from the digital world that are tending to spread into the space sector and transform its production model to cut costs, in addition to the use of "off-the-shelf components".[12] These business models are known as "Space as a service".

SaaS (Software-as-a-Service) is a well-known business model in the digital sector, which consists of providing software solutions over the Internet without having to install or own them, by means of cloud. This enables end-users to make use of the software solutions deploying them rapidly and using them only when they need them. Companies in the space sector have therefore drawn on this type of model to offer their customers satellite-delivered services such as space imaging, without the need to invest in a fleet of satellites. This not only gives customers access to a tailor-made solution - for example, changing the area to be imaged in near-real time, or changing the type of imagery (from optical to radar) but also reduces costs, as offered by the imaging company Spire.[13]

The second business model to emerge from the digital world, which is tending to develop in the space sector, is that of "platform as a service" (PaaS). PaaS is a cloud computing model that provides customers with a complete cloud platform (hardware, software, and infrastructure) to develop, run and manage applications and avoids the costs, complexity and rigidity associated with creating and maintaining this platform on-site. The PaaS provider hosts all infrastructure and development tools in its data centre. Typically, customers pay a fixed fee for a set quantity of resources or opt for pay-as-you-go pricing to pay only for the resources they use. This distinguishes it from the software-as-a-service (SaaS) model, where the same application is made available to numerous end-users. In the space industry, PaaS means enabling customers who want to develop a new "application" or run their own application to use the complete architecture of a space system (ground segment, onboard segment, and links), without having to invest in or maintain a complete system.

The latest business model to emerge from the digital world is Infrastructure-as-a-Service (IaaS). IaaS provides users with physical infrastructures, virtual machines, storage, networks, and firewalls, hosted by a cloud service provider. IaaS comes without the management costs associated with maintenance. In this model, users manage their own applications and data. As a result, the user doesn't need an on-site data centre and doesn't have to worry about physical upgrades or maintenance of these components.

In most cases, the IaaS user has full control over the infrastructure via an API[14] or a dashboard. In the space sector, this means, for example, providing the complete infrastructure to operate a constellation. In this case, the supplier can offer a hub on a satellite platform,[15] enabling the customer to host any type of payload, as proposed by Loft Orbital.

[12] Standardized products available in the mass market.
[13] Joel Spark, Space-as-a-Service (SPaaS) - the next generation of space-based business, 2022
[14] An API (Application Programming Interface) is a software solution that enables two applications to communicate with each other.
[15] Satellites are made up of two parts: the payload, which carries out the mission, and the platform, which ensures the satellite's operation by supplying it with electrical power, computing power and so on.

The logic of New Space has spread more or less widely without being directly copied. We can observe in the space industry of European Union member states a phenomenon of public policy convergence and an attempt by a certain number of companies to adopt this type of model in numerous European projects such as IRIS²,[16] or the datacentre projects in space (even if the latter seem little aware of the interest they represent).[17] In November 2022, the European Commission awarded Thales Alénia Space a feasibility study with the primary aim of reducing the carbon footprint.[18]

In a similar vein, China is keen to develop an "integrated space-earth information system", to make terrestrial (fibre optics, 5G) and space (broadband constellation and, in the near future, quantum communication satellites) communication networks interoperable, as Marc Julienne points out.[19]

On a slightly different note, India's space policy focuses on the development of space technologies, primarily to contribute to the country's development21 through mapping, communications and resource management,[20] while at the same time emphasizing the concept of frugal innovation.[21] As a result, start-ups are emerging with projects involving digital technologies such as artificial intelligence, like Newspace Research & Technologies or Blue Sky Analytics even if this remains a marginal phenomenon.[22]

Finally, at the opposite end of the spectrum, we find space policy struggling to find its own dynamic, and even more so to fit into a New Space logic. Despite the creation of Skolkovo, as Isabelle Sourbès- verger points out,[23] Russia faces numerous problems in terms of investment, industrial policy, and the supply of electronic components. Despite Russia's stated ambition to become a more powerful player in both the military and civilian spheres, it is hard to see how the country can modernize and digitize its space technologies under these conditions.

The space sector therefore seems to be strongly influenced by digital players, both in their approach and in their practice

[16] Iris² is a European constellation project designed to provide secure connectivity throughout the European Union, particularly in areas with low Internet speeds.
Louis de Briant, « L'Europe lance son projet de constellation spatiale souveraine », l'Usine nouvelle, 2022

[17] Ryan Morrison, « The European Union - and Big Tech - want to move data centers into space », techmonitor, 2022,

[18] The project is ASCEND Advanced Space Cloud for European Net zero emission and Data sovereignty. ASCEND: Thales Alenia Space to lead European feasibility study for data centres

[19] Marc Julienne, « La Chine dans la course à l'orbite basse. Perspectives on the future Guowang internet constellation », Asie.Visions, n° 136, April 2023

[20] Isabelle Sourbès-Verger, « China, Russia, India, Japan: essai de typologie de leurs ambitions spatiales en 2019».
Annales des Mines - Réalités industrielles, 2019.

[21] Frugal innovation is the process of meeting a need in the simplest, most efficient way possible, using the least amount of resources. It is often summarized as providing quality solutions at low cost, or innovating better with less.

[22] Sudeshna Mitra & Hemant Kashyap, « To Infinity & Beyond : Meet The 20 Spacetech Startups Winning The Space Race For India », Inc42 Media, 2024

[23] Op. cit

4. A space sector benefiting from digital development.

In order to ensure the viability of the business models promoted by digital players, today's satellites are increasingly carrying payloads that require significant processing or calculation capacities, particularly in the fields of earth observation and telecommunications. As a result, there is a growing trend towards the digitization of satellites. Satellites are thus becoming more complex, and more and more like "computers", whereas before a satellite was mainly made up of electronic cards programmable via RTEMS software.[24] This trend is set to increase with the development of cloud computing systems (mentioned above), autonomous navigation and on-board decision-making. At the same time, a miniaturization phenomenon based on distributed systems is driving the development of ever-smaller, ever-more powerful satellites, albeit with reduced volumes and electrical power.

Similarly, we can note the emergence of on-board systems involving artificial intelligence via neural compression systems and enabling on-board digital processing in an edge computing logical.[25]

To meet this challenge, increasingly high-performance components of the System on Chip (SoC)[26] type are being used, some of them optimized to support artificial intelligence algorithms, and more particularly so-called neuromorphic processors.[27] To deliver higher performance with lower power consumption, especially for short missions in low-Earth orbit, these new types of satellites are even more using processors and video components found in conventional computers. Initially reserved for demonstration missions, these components are increasingly used on commercial missions with small platforms. Examples include the Intel Movidius Myriad 2 processor on ESA's phi-sat-1 mission,[28] and the Intel Neuromorphic Loihi processor on NASA's TechEd 13 mission.[29]

We can therefore hypothesize that space technologies seem to be starting to use more conventional technology to ensure lower production costs, while at the same time increasing the complexity of the missions assigned to satellites. However, space technologies continue to use on more specific digital technologies, such as optical links or quantum technology, which are part of the digital world insofar as these technologies are integrated into existing information systems. For example, the emergence of reprogrammable satellites is being observed due to the development of FPGAs[30] or components running on Linux software.

[24] RTEMS software is operating software for electronic components such as processors or SOCs.
[25] Edge computing is an optimization method used in cloud computing, which consists of processing data at the edge of the network, close to the data source. In the space case, it enables very large data flows to be processed while saving on the bandwidth provided by the links.
[26] These are electronic chips containing complete integrated systems.
[27] These are processors whose architecture attempts to replicate that of the brain in order to optimize certain types of calculation.
[28] Φ-sats programme », ESA, 2022. Available atl https://philab.esa.int/flagship-programmes/phi-sats-programme/
[29] Marcus Murbach and al, « TechEdSat-13: The First Flight of a Neuromorphic Processor », NASA, 2022 https://ntrs.nasa.gov/citations/20220005780
[30] FPGA (Field-Programmable Gate Arrays) are logic integrated circuits that can be reprogrammed after manufacture.

As far as optical links are concerned, the ability to transfer very large quantities of data has become extremely important for both government and commercial missions. Until very recently, these links were provided by radio frequencies, but with the development of mega-constellations, some of the most sought-after frequencies became very congested. With the development of optical transmissions, operators now have access to much higher data rates. As an example, optical communications links can deliver up to 100 Gbps for both inter-satellite and ground-edge links.

Last but not least, the emergence of quantum technologies is primarily aimed at securing links, despite these having some vulnerabilities.[31] The quantum key exchange protocols[32] based on the non-cloning theorem guarantee that it is impossible to create a replica of a particle (a photon) in an unknown state. The realization of a quantum key exchange is therefore based on the ability to rapidly produce quantum objects in a prescribed state, measure them and transfer them. However, there are still very few devices in development, most of them being demonstrators and limited to low-Earth orbit, since beyond 1,000 km, problems linked to the quantum entanglement of the emerging photon.

These technical upheavals are profoundly transforming space technologies. On the one hand, they are greatly increasing the technical capabilities of space systems, which in consequence is making them more efficient by enabling them to process larger quantities of data and improving the way they are processed. For example, in the military sector, this could mean the ability to detect military ships operating at sea, thanks to the use of artificial intelligence, or the capacity to better protect telecommunications. In the civilian sector, it could mean more effective space applications for climate change analysis.

On the other hand, these transformations also appear to be profoundly transforming space systems, insofar as their capacities are increasingly being integrated into different information ecosystems that communicate with each other and could ultimately relegate space systems to the status of simple peripherals of cyberspace.

[31] Quantum communications are, for example, particularly vulnerable to denial-of-service attacks, especially as this involves stopping the communication to send back a new key, so the adversary can disrupt the communication channel by multiplying read attempts.
[32] There are two main quantum key exchange protocols, BB84 and E91.

5. The digitization of space is creating new security challenges and accentuating existing rivalries.

The digitization of space technologies represents a major new challenge, insofar as it is profoundly transforming the way we think about space security, by modifying the typology of threats and broadening the range of players in the field of space security. Historically, anti-satellite weapons were developed during the Cold War, in the context of nuclear tensions. The main aim was to deprive adversaries of their observation and warning capabilities, in order to optimize the effectiveness of their nuclear weapons. From the early 1960s to the early 1970s, the Americans and Russians began to think about missile defences, which were later transformed into anti-satellite weapons, as well as interceptor satellites. These different types of kinetic anti-satellite weapons are generally difficult to implement since they must take into account the constraints of celestial mechanics, which make "hit to kill" particularly difficult to master.[33]

In addition, the Anti-satellite weapons (ASAT) type had limited discretion since it remains detectable by early warning devices or sky observation capabilities (radar). Moreover, they were relatively expensive to develop, and the strategic options they offer are extremely limited, being confined to the destruction of the spacecraft or ground station. This meant that only the most powerful countries were in a position to possess this type of weapon.

Then, at the end of the 1970s, new anti-satellite weapon systems based on electronic warfare[34] appeared. The advantage of these weapons is that they can be used either directly from space or via satellite antennas which can be modified to jam satellite links[35] or inter-satellite links. Among electronic warfare weapon systems, we can also distinguish a sub-category: directed energy weapons. Their aim is to provoke successive heating or electromagnetic overloads, either by lasers (Light Amplification by Stimulated Emission of Radiation) or by masers (Microwave Amplification by Stimulated Emission of Radiation) which emit a coherent beam of microwaves.

These new weapon systems based on electronic warfare have changed the old logic of ASAT as they have expanded the range and effectiveness of the available strategic options. These allow spying, disrupting, temporarily or permanently interrupting the services provided by a satellite and are extremely difficult to dodge. However, they are complex to use. In the case of directed-energy weapons, a direct line-of-sight to the target is required, which is difficult to achieve given that the average speed of a satellite is around 8km/s. This adds additional constraints for concealing attacks all the more, their development cost is

[33] That's why all these weapons have explosive charges, despite the fact that they are classified as kinetic weapons.
[34] According to the CICDE glossary (updated 2015) electronic warfare is any: "military action designed to exploit the electromagnetic spectrum, encompassing the search, interception and identification of electromagnetic emissions, the
[35] This applies both to the links containing the data supplied by the satellite, and to the links used to operate the satellite.

rather high and their implementation on the space segment necessarily requires space capabilities reducing their uses mainly to space powers.

More recently, we have seen the emergence of a new category of threat to space systems, in addition to the classic ASAT and electronic warfare methods, namely cyberattacks. Cyberattacks have the advantage of being easier to implement, since most of the complications associated with space mechanics can be avoided, with the exception of those relating to the capture of satellite links. They are also more difficult to trace due to the presence of obfuscation techniques and are less costly to implement, which necessarily has consequences for the typology of players in the field of space security. Indeed, cyberthreats further expand the strategic options available to governments, giving them the ability to target any segment (and potentially at the same time). The segment links the object of attack and, more specifically, the data that can be altered through man-in-the-middle attacks.[36]

They can also be used to carry out more conventional attacks against the ground or space segment (espionage, disruption, temporary or permanent interruption). Furthermore, cyberattacks have the advantage of being more discreet than missile launches, which remain relatively detectable by radar, and require special know-how and technical resources to implement. So that only states with space or ballistic capabilities could have access to this type of weaponry. This considerably narrowed the field of potential aggressors, but from the early 2000s and the emergence of New Space, the field of space security players changed considerably, bringing in not only economic players from the digital world but also malicious actors.

Those involved in the security of space systems will therefore find themselves confronted with security issues specific to IT, which were previously limited. As in the case of cyberattacks on conventional information systems, the question of satellite cybersecurity and its vulnerability[37] does not really differ from the more common cyber-physical systems.[38] Thus, in the case of the ground segment, Demilitarize zones (DMZs)[39] are used to decouple them from the Internet and firewalls. Various security and system access management policies also apply, as do a range of information system protection standards not specific to the[40] space segment. From the point of view of vulnerabilities, there are also human vulnerabilities linked to "social engineering" techniques such as phishing, as well as flaws linked to a lack of vigilance on the part of operators or non-compliance with security procedures (e.g., use of USB keys outside the white station). To these must be added software security flaws, such as zero-day vulnerabilities[41] and, more generally, all attacks on industrial control systems (ICS), as the operation of the ground segment can be perceived, from a cybersecurity point of view, as an industrial system.

[36] ANSSI defines a man-in-the-middle attack as "a category of attack where a malicious person interposes himself in an exchange in a way that is transparent to users or systems. The connection is maintained, either by substituting the transferred elements or by reinjecting them. A well-known attack in this category is based on the compromise of ARP tables (ARP Poisoning). Countering attacks from the middle is also one of the objectives of key management infrastructures.

[37] A computer vulnerability is a security flaw in an information system, application, software or even a hardware component. These security flaws can also come from users and the way they use their IT tools.

[38] Cyber-physical systems are systems of computer entities collaborating with each other and interacting with the physical world via sensors and actuators. They can take many different forms, such as industrial systems, aircraft engines, autonomous cars and so on.

[39] DMZ or Demilitarize zone, in IT it's a subnetwork isolated from the Internet and a secure local network, acting as a sort of buffer zone and able to contain machines that don't need access to a secure local network.

[40] With the exception of the NIST IR 8401 standard, released in 2023, which proposes a framework for optimizing risk management dedicated to the ground segment.

[41] 44A zero-day vulnerability is a software vulnerability detected by cybercriminals before the vendor is aware of it. Because vendors are unaware of this vulnerability, no patches exist, and attacks have a high success rate.

Today, those involved in space security have to deal with potential attackers who have a different rationale from that of states, such as cyber-criminals,[42] cyber-mercenaries or hacktivist groups, who can use both propaganda and technology to camouflage their communication networks.[43] We also need to take into account states with no space capabilities or low ballistic capabilities, which can now become potential attackers through cyberspace and the interconnection it produces with space technologies.

Two particularly interesting cases stand out in this respect. The first concerns attacks perpetrated by the cyber-criminal group Turla.[44] This group is known in part for exploiting flaws in satellite networks to conceal the transfer of data resulting from their espionage campaign targeting embassies, administrations and companies, using downlinks which are often poorly protected.[45] The second case concerns the experiment carried out by Professor Todd Humphrey of the University of Texas, who hijacked a boat by spoofing a GPS signal.[46] These two cases teach us two things. The user segment now appears to be a particularly interesting target for malicious actors, which means that it has to be treated differently from the ground segment.

All this contributes to the creation of asymmetrical relationships in an environment where interactions were previously the domain of states. What is more, the emergence of new players makes it even more difficult to attribute attacks. It therefore becomes very complex to know whether the attack is the work of a state, a non-state actor or a state hidden behind a non-state actor, as could be the case with Turla.

However, this does not prevent long-standing rivalries from persisting. From the outset, space has been perceived as a strategic marker reflecting political and economic rivalries on the ground, as Isabelle Sourbès-Verger points out.[47] The digitization of space activities and technologies seems to fit into this logic of rivalry, which is both old and new, through the competition between economic players.

Digitization plays an important role in the emergence of new defence space policies, space domain awareness being one example. This is based on a logic of complementary layers enabling the acquisition and processing of space-based information. However, for it to work, it requires on-board processing capabilities (edge computing), as data flows are too large to bring them all down,[48] as well as detection capabilities provided by artificial intelligence, the development of large-scale connectivity and quantum technologies to secure them, and "as a service" business models to reinforce legacy military capabilities. This brings us back to the very classic logic of mastering the information and sovereignty chain, fully in line with the "information superhighway" already envisaged in the 1990s with the birth of the RMA, as Xavier Pasco points out,[49] with space technologies becoming an information infrastructure.

Similar approaches can also be found in China, where various digital technologies are integrated into a wide range of dual-use capabilities. This logic applies both from an economic development perspective -

[42] Lev Grossman, « Did Hackers Hijack a British Military Satellite? », Time magazine, 1999
https://content.time.com/time/magazine/article/0,9171,20673,00.html
[43] D. Housen-Couriel, , "Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses", Law & Cyber Warfare, 2015
[44] This group is supposedly linked to Russia, but in the absence of precise attribution, we'll treat them as cybercriminals.
[45] S. Tanase, September 9, 2015, "Satellite Turla: APT Command and Control in the Sky", Kaspersky website
https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
[46] M. L. Psiaki, T. E. Humphreys and B. Stauffer, August 2016 "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," in IEEE Spectrum, vol. 53, no. 8, pp. 26-53
[47] 50Sourbès-Verger, I. (2022). Space, a special place for political and technological rivalries. Revue Défense Nationale, 851, 73-78.
[48] Hence the interest in edge computing and the development of optical links.
[49] Xavier Pasco. « New forms of competition in space ». Revue Défense Nationale, 2022.

the sale of Ground segment-as-a-service[50] in Greenland being a perfect example. But also, to blur the distinction between civil and military systems in the event of conflict, duality being part of their defence doctrine.[51]

On the economic side, apart from the competition for market share, the digitization of space technologies will necessarily lead to competition for the establishment of norms and standards for the interoperability of different information systems, this is similar to what happened with 5G, where American and Chinese systems are the most developed, forcing their partners to equip themselves with their technologies, which are subject to their control, notably through the ITAR treaties.[52]

[50] Ground segment made available for a fee and remotely accessible.
[51] Marc Julienne, « China's ambitions in space the sky's the limit », Ifri, 2021
[52] ITAR (International Traffic in Arms Regulations) is a U.S. regulation that controls the manufacture, sale and distribution of defense and space-related items and services.

6. Conclusion:

The space sector therefore seems to be facing a digital transformation as we observe increasingly digitized space technologies and practices imported from the digital world into the space sector. This trend is becoming increasingly widespread among the world's leading space powers, even if their development appears uneven.

However, the digitization of space technologies may well result in the loss of the specificity of space technologies (with the exception of scientific activities) in favour of a simple infrastructure for an information society, with a generalization of the classic problems associated with the digital world.

The emergence of these new digital technologies in the space sector must be taken into account when considering space traffic management and space situation awareness, as they are likely to develop further in the near future.

This integration of space and digital technologies is also creating new security challenges, with the multiplication of cyber threats and the diversification of malicious actors with their own logic and interests. Added to this are traditional state rivalries, both strategic and economic, making the perception of the space ecosystem even more complex, all the more so as it has become virtually indispensable to the smooth running of many vitally important business sectors.

This new geopolitics of space requires us to think about new regulatory instruments and collective security mechanisms, insofar as issues specific to digital technology are added to those of space. In the same way, the promotion of norms and standards by States for these new technologies must be at the heart of these new geopolitical concerns, as they have an impact on the sovereignty of States.

Finally, this new geopolitics of space should also lead us to question the place of these new players operating between the civilian and military worlds, and who may now potentially be the subject of legitimate targets under international law, since they become in part the support of military activity through the provision of services to armies.

Acknowledgements

Il presente paper è stato realizzato nell’ambito del progetto “Geopolitica del Digitale”, promosso dalla Fondazione Med-Or, in collaborazione con il Center for International and Strategic Studies (CISS) della Luiss Guido Carli, grazie al sostegno della Fondazione Compagnia di San Paolo all’interno del bando “Geopolitica e tecnologia.

About Luiss School of Government

The Luiss School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions. The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organizational leadership).

For more information about the Luiss School of Government and its academic and research activities visit. www.sog.luiss.it

Luiss
School of Government

Via di Villa Emiliani 14
00197 Roma
T +39 85 225052
sog@luiss.it