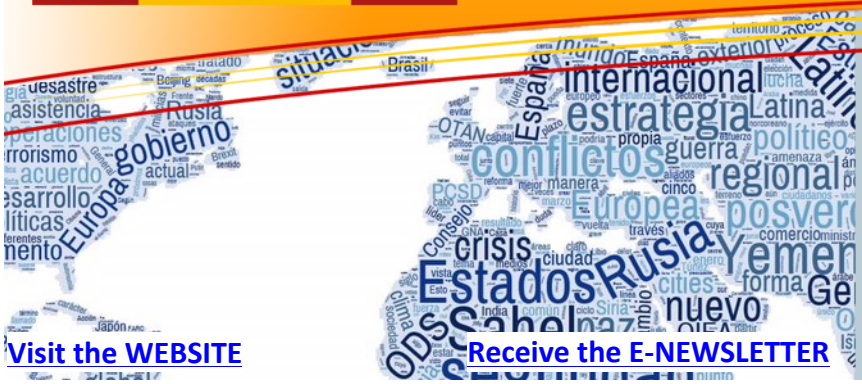
ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Paper

71/2022 16/11/2022

David Ramírez Morán

Global communications of private nature



Global communications of private nature

Abstract:

Private providers are behind services as important as social networks and satellite communication systems, providing the services on a global centralized scope.

It's about services that, currently, support the new relation model established at all the levels, from the citizen to the international organizations. The importance of the cognitive domain, both in international relations and in conflicts, has gained even more importance under this new model. So, the access to these technologies has become strategic and critical simultaneously.

The private nature of the businesses that provide these services poses a defiance to face questions such as sovereignty and geopolitics, given the different existing relations between states, services providers and users.

Keywords:

Global communications, social networks, sovereignty, private enterprises

Comunicaciones globales de naturaleza privada

Resumen:

Detrás de servicios tan importantes como las redes sociales o los sistemas de comunicación por satélite hay proveedores que prestan los servicios de forma global y centralizada.

Se trata de servicios que, en la actualidad, sustentan el nuevo modelo de relación que se ha establecido a todos los niveles, desde el ciudadano a los Estados. La importancia del dominio cognitivo, tanto en las relaciones internacionales como en los conflictos, ha ganado aún más fuerza bajo este nuevo modelo. Es por ello que el acceso a estas tecnologías se ha convertido simultáneamente en estratégico y crítico.

La naturaleza privada de las empresas que prestan estos servicios supone un reto para abordar cuestiones como la soberanía y la geopolítica ante las diferentes relaciones existentes entre los Estados, los prestadores de los servicios y los usuarios.

Palabras clave:

Comunicaciones globales, redes sociales, soberanía, empresa privada.

How to cite this document:

RAMÍREZ MORÁN, David. *Global communications of a private nature*. IEEE Analysis Paper 71/2022.
https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA71_2022_DAVRAM_Comunicaciones_ENG.pdf and/or bie^3 link (accessed on day/month/year)

Introduction

The evolution of information and communication technologies has taken place in a very short period of time. Services that only a few years ago were unimaginable even to technologists are now a reality which, aside from being widely available on the market, is also enhanced by the network effect. An increasing number of services are being provided by private companies on a global scale thanks to factors such as internet connectivity and the use of satellite systems that provide global coverage with the same investment needed to obtain regional or local coverage. These companies aim to reach a high volume of users in their search for business, which also contributes to the network effect. More users also means more information available to work with in today's scenario, where data are the raw material and the use of artificial intelligence that works with them is spreading.

The phenomenon of social networking is a clear example of this evolution. Social networks have displaced other media for various reasons, including the immediacy, accessibility and interactivity they provide to the user. The information dissemination capacity they provide and the limited control that can be established over this capacity pose a number of challenges. Users are increasingly dependent both for interpersonal communications and for obtaining information previously obtained by other means. In parallel, the volume of users that can be reached also makes this technology a medium for uncontrolled communication, opinion generation, manipulation and even the dissemination of false information in a self-serving manner. There are several countries which, either because of their ideology or because of conflicts that have arisen in their territory, set specific or permanent limitations on access to social networks to stifle the loudspeaker they are or to limit the information that can reach users.

All this digital revolution and the benefits to society it brings would not be possible without reliable connectivity and sufficient capacity. Fixed infrastructures, first copper and then fibre, are being displaced in many scenarios by wireless connectivity. Even though 5G technology, which is in the process of being deployed, provides the necessary capacity, achieving universal availability is nonetheless a very complex issue. There are environments where the deployment of fixed, mixed or wireless infrastructure is economically unfeasible, and it is these places that prompted the consideration of systems providing high-capacity connectivity with global coverage. Satellite was the solution to the problem of making this service available to all or almost

all of the world's population. Initiatives to develop these solutions have come from the private sector and several solutions are already available or are on the horizon[1]. The first commercial product has been provided by Starlink[2], a company owned by Elon Musk, which aims to deliver global internet connectivity via satellite.

Private service models

Implementing a global system that knows of no borders does not fit well with the developments of a state public administration in terms of its powers. There are exceptions in this respect with systems which, although conceived locally or regionally, have been extended to global use. The system for assigning addresses and managing domain names arose out of the need for this service at the dawn of the internet and is now managed by a US non-profit company, ICANN. The GPS satellite radio navigation system also started as a US military system and, although it is still publicly provided, is now available to the world's population

But it is not only technological progress that is behind this transformation. One must also look at economic structures where private companies have capitalisations greater than the wealth of many countries. These corporate giants have far greater investment capacity and flexibility than governments, allowing them to embark on very long-term projects driven purely by economic interests and less influenced by political decisions.

Technological developments and new business models have transformed the landscape. Private initiative now has means that were formerly only available to the public sector, such as access to space. Having this capability means that in a competitive environment it needs to be exploited, which has led to a revolution in the criteria applied to determine the viability of systems that were previously prohibitively expensive. New business philosophies have also contributed to the creation of systems that respond to much more ambitious objectives with a global mass reach.

[1] https://www.comoves.unam.mx/numeros/articulo/258/la-constelacion-starlink
[2] www.starlink.com

Global mobile communications

The need for mobile communication systems with global coverage was initially met by systems provided by private companies such as Iridium[3], aimed at very specific sectors due to the high costs associated with the complex infrastructure of a satellite-based system deployed more than thirty years ago. The niche product it provided drove the company into bankruptcy, but a new approach to the business subsequently allowed it to build on existing infrastructures to make a viable product which, for more than 25 years, has not only continued to operate, but investments are now being made in to keep it running and to add new functionalities.

OneWeb is another company that in 2012 likewise envisioned the business opportunity of a high-capacity satellite data communication system with global coverage. Like Iridium, it suffered a bankruptcy process in 2020, from which it emerged thanks to investments by the Indian company Bharti Global and the British government, which intended to use the satellites' capabilities to deploy its own global positioning system due to the forced abandonment of the European Union's Galileo system due to BREXIT.

From a different perspective comes Starlink, which aims to provide high-capacity, low-latency mobile internet connectivity to individuals anywhere in the world at an affordable price. It is a real technological challenge, one of the ingredients that characterise the sectors in which Elon Musk invests. Companies such as Tesla, which produced some of the first fully electric high-performance vehicles and is currently working on autonomous driving, or SpaceX, which seeks to reduce the costs of access to space with recoverable launchers, allow us to outline the criteria under which this communication network of astronomical numbers, like the thousands of satellites in orbit it requires, was launched.

Social media

Social networks are also a private initiative phenomenon that have rapidly transformed communication and generated a turning point in the dissemination of information. Their initial individual use gave way to the presence of organisations that used them both to distribute their information and to take advantage of the group phenomenon achieved with accounts' followers. Nowadays, they are one of the main sources of information for

[3] https://www.iridium.com/

a significant percentage of the population. In return, companies are collecting information that is useful for creating new products via targeted advertising and the generation of intelligence that can be of interest for product design or even for policy research.

Social networks have even become so popular that they have become loudspeakers for causes. They are tools that allow situations and events to be reported that formerly did not create even a ripple. They provide information almost immediately on issues of all kinds and without the filter that naturally existed in traditional media publications. Conflicts are quickly covered by the media across the different networks, providing a platform for publicity, and are used as tools for such things as convening or organising activities.

Limits to access to information

Governments may see internet access as a risk to state interests, especially ones that do not respect rights such as freedom of expression and freedom of information

The Great Wall, as the systems for limiting and filtering internet connections in the territory of the People's Republic of China are known, is one of the best-known examples of these practices. To preserve the interest of the state, the system prevents connection to certain internet servers, such as newspapers, blogs, etc. However, the system is not perfect and can be circumvented by using virtual private networks (VPNs), which encrypt connection information so that it cannot be identified by the filters. Nonetheless, these systems are also vulnerable themselves because, after all, the VPN must connect the user's computer to a server outside the controlled territory to access the restricted content and send it encrypted to the user. Filtering tools can identify the servers to which connections are made with measures as simple as deeming them inappropriate because they cannot identify the information being sent to them, thereby having reason to block them.

Measures less drastic than the above have also been taken by other countries.

During the so-called Arab Springs, several countries, such as Egypt, Libya, Syria, Bahrain, Tunisia and Saudi Arabia, restricted internet access to varying degrees for their citizens.

In February 2014 the Turkish government issued the Law No. 5651 on the Regulation of Internet Content[4], which allowed the government to block access to international websites for different reasons, including "protecting young people and the general public from harmful online materials". In the same year, in application of this law, access to Twitter was blocked for days. The blocking was easy to counter by simply configuring the computer to search other DNS servers as they only removed the entry for Twitter in the Turkish DNS, the yellow pages that convert the name of the website into the numeric IP address to which the computer must connect, and, to connect flawlessly, it sufficed to setup the computer to ask other DNS servers..

In the wake of the ongoing unrest in Iran following the death in a police station of the 22-year-old woman Mahsa Amini hit by a heart attack[5], the Iranian government has blocked almost all access to the internet due to the intensification of protests against it[6].

Russia is another country that has been filtering access to certain types of content and websites for years, and this practice has intensified in recent months since the invasion of Ukraine.

The invasion has also limited access to information because communications infrastructure has been severely affected by the fighting. Given the practices employed in previous Russian conflicts, when kinetic conflict was preceded by different types of cyber-attacks affecting technological and governmental infrastructures, a higher number of successful cyber-attacks against technological infrastructures was in fact expected. However, it has been the kinetic attacks that have most affected communication capacity on Ukrainian territory[7].

[4]WHITNEY, Lance. "Turkey approves legislation to block Internet sites" https://www.cnet.com/tech/tech-industry/turkey-approves-legislation-to-block-internet-sites/

[5]"Young woman who was arrested this week in Iran by the morality police for wearing the headscarf in the street dies" https://www.rtve.es/noticias/20220916/muere-mahsa-amini-detenida-llevar-mal-velo-iran/2402526.shtml

[6]Siladitya Ray. "Iran Blocks Nearly All Internet Access As Anti-Government Protests Intensify" https://www.forbes.com/sites/siladityaray/2022/09/22/iran-blocks-nearly-all-internet-access-as-anti-government-protests-intensify/

[7]CUBEIRO, Enrique, "El ciberespacio en la guerra de Ucrania " https://www.ieee.es/publicaciones-new/documentos-de-opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.html

Starlink in Ukraine

The use of existing telecommunication infrastructures during the conflict in Ukraine has posed a risk because it allows the origins of broadcasts to be traced through radio frequency signals[8] and also the content of communications to be intercepted. The fact that the networks are remaining operational during the conflict has been the object of various justifications, including the effort put into it by the Ukrainian government, the collaboration between the different Ukrainian suppliers, external collaborations and even the use that the Russian forces are making of the systems vis-à-vis the technical difficulties and lack of equipment that have been blamed on them in different forums.

The communications service provided by the Starlink system is a communication tool for the Ukrainian population given the destruction of the terrestrial infrastructures that provided both wired and wireless services. Thanks to the outpouring of foreign collaboration, the provision of Starlink terminals free of charge to help inform the population about developments in the conflict is a further asset. The company has financed both the 20,000 or so handsets that have been shipped to Ukraine and months' worth of the associated monthly costs to the tune of around $80 million, besides an estimated additional $20 million in spending by the end of the year. Faced with this amount and the associated costs of the system: $120 million until the end of the year and $400 million over 2023, the company contacted the US administration requesting financial support[9], but eventually stated that the service would not be discontinued regardless of the government's response[10].

Russia has taken the next step in face of the growing use of Starlink technology to regain communications capability on Ukrainian territory. In a statement by Konstantin Vorontsov, deputy head of the Russian delegation to the UN, he highlighted how this civilian infrastructure is being used for military purposes[11] and can therefore be considered a military capability, meaning that measures could be taken to disrupt its operation. The characteristics of the system make tampering by electromagnetic means

[8] Kieran Devine Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595

[9] MARQUARDT, Alex. "Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab" https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine

[10] IBRAHIM, IM. "Elon Musk says SpaceX won't turn off Starlink satellite regardless of Defense Department funding" https://edition.cnn.com/2022/10/24/politics/elon-musk-spacex-starlink-us-funding/index.html

[11] VIGLIAROLO, Brandon. "Russia says Starlink satellites could become military targets" https://www.theregister.com/2022/10/28/russia_raises_possibility_commercial_sats_strike/

very complex. However, the infrastructure of the system, including the various satellites in orbit, can become military targets for Russia. Attacking these systems, whether with traditional shoot-down, electromagnetic or logic weapons, poses a serious risk to all countries. Satellites are prepared to have a lifetime within a somewhat longer potential life cycle. After their useful life, they have mechanisms that take obsolete or damaged devices out of useful orbit and into a temporary orbit that leads to re-entry into Earth orbit for destruction by atmospheric grazing.

Damaging one of the devices in a logical way can completely alter its functions. This may result in loss of control over the device and the inability to perform orbit correction manoeuvres, either to return the device to orbit or to take it out of orbit.

The device's physical destruction is one of the most serious potential problems as the debris resulting from it could damage other space devices passing close by or crossing the orbit where it was located. The arrangement in orbital planes of the multiple satellites required by the system greatly increases the likelihood of debris from one destroyed device affecting other devices in the same orbit, triggering a chain reaction that could render the orbit totally unusable for any future space use.

Starlink in Iran

The particular case of Iran regarding the Starlink communications system is a situation worthy of detailed analysis.

Due to bans on the sale of certain products to Iranian nationals, the service provider did not initially allow users to make purchases when the country of residence was Iran. The protests mentioned above led the Iranian government to shut down access to major social networks by limiting the possibility of connecting to them through Iranian infrastructure. From outside the country, however, it was proposed that the Starlink service should be able to serve Iranian citizens so that the outside world could know what was happening there. In fact, it was the White House itself that approached Elon Musk about the company also providing the service in Iran[12]. The American company authorised the contracting of the service to Iranian nationals, leading to information

[12]"White House in talks with Musk to set up Starlink in Iran - CNN" https://www.reuters.com/technology/white-house-talks-with-musk-set-up-starlink-iran-cnn-2022-10-21/

beginning to leak out about the clandestine introduction of terminals into Iranian territory[13].

The fact of the company authorising the use of its systems on Iranian territory may pose a number of problems. The first is that a service is being provided in a territory subject to international sanctions that impose limitations on the sale of certain goods and services to its nationals. The characteristics of the communication service provided by Starlink would bring it within the framework of these sanctions, meaning that the service provider, precisely by providing the service in that territory, could be in breach of the sanctions. Moreover, given that it is a private service that is not free of charge, the company must receive payments from users, which may also contravene bans on the movement of capital by nationals of that country.

From the local point of view, if the use of the frequencies used by the system is not authorised, it is a source of risk for users, meaning their possible sanction. In turn, if the system is used as a measure to contravene state-imposed limitations, users enter an environment of secrecy that can potentially be used to both target and prosecute them on charges far beyond the mere technical violation of state regulations.

From a geostrategic point of view, the system becomes a geopolitical tool whereby the country in which the supplier company is located is affecting the interests of the state in question.

Getting the system into use on Iranian territory is not easy for a number of reasons. First, it uses specific terminals that must be made available to users[14]. Customs mechanisms could be put in place to prevent the entry of these terminals into Iranian territory. Only those arriving via alternative logistics routes could reach their destination. Access to these routes may be costly, limiting the profile of users with access to this route. This dilutes the justification of giving a voice to activists defending causes against the state since this population profile does not usually correspond to those who can afford the costs and risks of resorting to this means of having a voice.

[13]MURPHY, Aislinn. "Elon Musk opening up Starlink in Iran " https://nypost.com/2022/09/24/elon-musk-opening-up-starlink-in-iran/

[14]WOOLLACOTT, Emma. "Starlink Terminals Smuggled Into Iran - But How Effective Can They Be?" https://www.forbes.com/sites/emmawoollacott/2022/10/25/starlink-terminals-smuggled-into-iranbut-how-effective-can-they-be/

Starlink signal for GNSS

The acronym GNSS, which stands for Global Navigation Satellite System, has for many years been directly associated, at least in the western hemisphere, with the American Global Positioning System, GPS. The European Union recognises the importance of this technology, relying on the Galileo programme to autonomously count on this positioning and time reference capability, as well as other additional functionalities of interest for defence and security.

According to a University of Texas study[15] in search of a GPS backup, carried out with funding from the US Army, the signal transmitted by Starlink satellites could be used to accurately determine the location of receivers in the same way as it is done with dedicated GNSS systems, such as GPS and Galileo.

A GNSS system relies on the receiver being able to determine the relative delay with which signals from each of the satellites within its field of view reach it. If the precise location and velocity of the satellites transmitting the signal are also known, the position of the receiver can be determined by solving the corresponding equations.

In the signal transmitted by Starlink's satellites there are beacons or reference signals which, without the need to access the private and confidential information of the system's users, allow these delays to be accurately determined thanks to its high bandwidth. Moreover, in the case of Starlink, because the satellites are in a low orbit just over 500 km above the ground, their position relative to the receiver varies very rapidly. This is why to inform about the satellites that are visible at a particular location from the receiver and to facilitate signal acquisition, the location of the satellites is announced periodically and publicly.

The paper proposes that the accuracy of the system could be improved by incorporating information on the drift of the synchronisation reference clocks on board the satellites into the system's navigation message, which is sent in the satellite signals. This would reduce the positioning error obtained from the received signals from the theoretical thirty metres provided by the current signal to an error of just a few metres. Concurring with the researchers responsible for the paper, this would require a simple modification of the software that governs the operation of the satellites so that this correction value is sent to the receivers with a certain frequency.

[15] HARRIS, Mark. Starlink signals can be reverse-engineered to work like GPS - whether SpaceX likes it or not. https://www.technologyreview.com/2022/10/21/1062001/spacex-starlink-signals-reverse-engineered-gps/

The proposal made by the researchers was initially welcomed by company executives, although they later attributed to Elon Musk himself the words that would halt the initiative: "Every other LEO [low Earth orbit] communications network has gone into bankruptcy...so we [SpaceX] have to focus entirely on staying out of bankruptcy. We cannot afford any distractions".

Despite the feasibility of implementation, whether it is useful when put into practice is also questionable. Starlink operates in the X-band radar frequency, between 8 Ghz and 12 Ghz. Receiving signals in this band requires bulky antennas, especially when compared to the ones only some centimetres on their side required for a GPS receiver whose signal is in the L-band at 1.575 Ghz.. The antennas provided by Starlink for its system are just 30 by 30 cm in size and weigh a few kilos.

Conclusions

Private initiatives are transforming the international scene in times of conflict and peacetime alike. New infrastructures in the hands of private companies and whose direct control escapes the states are becoming tools that can be strategic and critical. The service they provide may be global and, under this circumstance, the asset may be strategic locally, for the service provider, externally or simultaneously in a combination of two or more of the situations described above. Because they are strategic in achieving certain objectives, they consequently become strategic targets to be attacked in the event of armed conflict to limit or eliminate the capabilities they provide. This international nature may result in attacks against them implying, in the context of a given conflict, the need to attack the interests of third parties who could potentially be directly involved or not in the conflict.

In the case of satellite systems, where the main infrastructure may consist of the elements in orbit, an attack affecting the operation of the system can be addressed using different approaches. The terrestrial and/or aerospace sector can be targeted. In the case of physical attacks, the special characteristics of the objects in orbit may result in the attack achieving the desired objective of stopping the service, but at the cost of irreversible consequences such as the disabling of orbits due to the generated debris, harmful to any other element located in the same orbit.

Services like social networking or mobile satellite communications are being deployed by private companies. Far from curbing diplomatic conflicts, the governments of the companies' countries of residence may be subjected to accusations because of the actions the companies are carrying out in foreign territories. The capabilities that these services provide in today's world make them useful tools for dealing with conflict and may lend themselves to voluntary use against the interests of other countries. Cooperation between governments and companies further contributes to blurring the boundary between public and private interests, making it more difficult to differentiate between civilian and military use of the systems in case of conflict.

Even with collaborative initiatives between governments and business, the latter does not have to accommodate requests that deviate from their strategic and commercial interests to respond to a state need. To this effect, a very close relationship between the industrial fabric and the government is necessary so that, in cases of need, both parties make better use of the capabilities available for a country's defence and security interests.

*David Ramírez Morán**
IEEE Senior Analyst
@darammor