Advances in Military Technology
Vol. 16, No. 1, 2021, pp. 133-147
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01409

Space Systems as the Weakest Link

S. Dygnatowski[*]

Aeronautics Faculty, Military University of Aviation, Dęblin, Poland

The manuscript was received on 17 April 2020 and was accepted
after revision for publication as technical information on 7 June 2021.

Abstract:

Although it is widely believed that the space sector is one of the pillars of national security, in practice cosmic systems exist somewhat outside the area of critical infrastructure's discussion. Cybersecurity of space systems does not differ significantly from industrial cybersecurity, however, the uniqueness of the sector and space technologies means that its vulnerability to digital incidents depends on a number of factors that does not occur anywhere else. The purpose of the article is to defend the thesis that space systems are the weakest link in critical infrastructure systems, because the level of their cybersecurity is still disproportionate to the level of their technological advancement.

Keywords:

cybersecurity, cyberattacks, satellite systems, space systems, satellite technologies

1 Introduction

The space sector is considered to be one of the pillars of national security by both countries with the largest military potential, i.e. the United States and Russia, as well as the states endangered by a potential intervention from outside, i.e. Iran, Pakistan and Syria. From the military point of view, it is impossible for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – C4ISR) to function without accessing satellite data. Moreover, the use of satellite technology is of fundamental importance for the preparation and conduct of effective operations of armed forces. Currently in the inventories of the US military, there are over one million GPS receivers, from field troops to long-range cruise missiles [1].

The former commander of the 1st Space Brigade of the U.S. Army Space and Missile Defence Command/Army Forces Strategic Command Colonel Richard L.

[*] *Corresponding author: Aeronautics Faculty, Military University of Aviation. Str. Dywizjonu 303 no. 35, PL 08-521 Dęblin, Poland. Phone: +48 261 51 79 91, E-mail: s.dygnatowski@law.mil.pl*

Zellman noted that *the American war machine is becoming increasingly dependent on space technology and approximately 70 percent of the major weapons systems rely on signals transmitted from space* [2]. The world armies have understood that the military superiority of the United States stems from the undisputed access to the cosmic domain. The experienced officer in the US Army stresses that it is much cheaper and easier for the enemy to disrupt or damage a military satellite than to develop their own orbital platforms. Each state that has its own satellites and means to launch them may be capable of attacking the artificial satellites located on the low Earth orbit. Consequently, space systems have become objects of frequent cyberattacks, because their level of cybersecurity is still *disproportionate* to the level of technological sophistication of these systems. Moreover, cybersecurity challenges are unique in their essence, complicating equalization of digital capabilities with regard to the whole sector.

In view of the above threats related to the possibility of temporary or permanent unavailability of satellites, not only has the training of American soldiers in map reading or, in the case of naval personnel, navigation through the star system, been restored, but also, for example, work has begun in the US Agency for *Defence Advanced Research Projects Agency* (DARPA), operating within the structures of the US Department of Defence on a new generation of precision navigation that could work without GPS [2].

Although dominance in space was not a priority for the US National Security Strategy, presenting it in 2017, the US President, Donald Trump emphasized that the unrestricted access of the United States to the space domain is in their vital interest, and any disruption or attack on a critical infrastructure space element would meet with a purposeful reaction in the United States chosen by place, time, manner and domain [3].

It should be noted, however, that the US National Security Committee, as early as 2001, recognized the development and launch of deterrence and defence assets against hostile acts directed at US space objects considered to be one of the key issues [4]. The Committee's report indicated that the spectrum of threats in space is wide, and each of them has its unique features, development dynamics and distinctive measures to counteract them, being subject to permanent changes.

Threats or attacks on space capability can have national, economic and political consequences and may provoke global crises. These attacks can take different characters and forms and can therefore be divided into the following kinds of attacks:

- IT – all kinds of attacks in the digital domain on satellite handling systems are one of the elements of a wide spectrum of these threats, among others, alongside anti-satellite weapon (ASAT),
- conventional – directed at ground-based objects supporting satellite systems, interference from laser signals and systems or electromagnetic pulses capable of destroying or damaging satellites [5].

Although the opinions of international lawyers confirm that artificial satellite communications, navigation and remote sensing are not weapons (none of the agreements making up the international space law prohibits the use of satellite technology for military purposes) and these satellites mainly fulfil a supporting role for the armed forces of different countries, they can become weapon as a result of a deliberate cyberattack.

Bearing in mind the above, the author wishes to discuss cyber-attacks (and their potential consequences) on satellites and their ground infrastructure in this paper. Therefore, the author has analysed IT security incidents related to satellites or their ground infrastructure. The analytical method has made it possible to consider the analysed cyber-attacks in terms of solutions to the types and vectors of attacks and applied security measures. For this reason, it was necessary to discuss satellite technologies and the most common cyber-attacks on satellites in this article.

Moreover, in order to achieve the aims of the article, the author found it necessary to use press articles devoted to cyber-attacks on satellites and their infrastructure. The above-mentioned research method allowed the author to capture the issues and challenges related to the security of information and communication technology satellites.

2 Satellite Technologies

Satellite technologies are a type of space technologies. Most of today's satellites are used for communication, environmental monitoring or navigation purposes. In outer space, there are both governmental (including military) and commercial satellites [6].

2.1 Types of Satellites

Satellite communication:

Satellite communication, which embraces sending messages via electromagnetic systems, being an absolute basis for intercontinental and regional communications, is part of modern space technologies.

Satellite navigation:

The second pillar of space technologies is a satellite navigation system, which is based on three segments:

- the satellites which are evenly distributed on circular orbits around the Earth constitute the space segment,
- ground segment – the ground segment is made up of surveillance stations, observing each of the satellites in an uninterrupted manner,
- user – the user's receiver receives signals from many satellites, the exact position of which is known, compares these signals and on this basis calculates its own geographical position.

The best known navigation system known as Global Positioning System (GPS) is a constellation of 31 NAVSTAR (NAVigation Satellite Timing And Ranging) satellites orbiting at an altitude of 20 278 kilometres or 12 600 miles in six orbital planes.

2.2 Satellite Remote Sensing

The third pillar of space techniques is satellite remote sensing, which is also composed of three segments: cosmic (including space infrastructure, allowing the acquisition of satellite data from the satellite level), ground (ground-based infrastructure measurements) and service (infrastructure of delivering data).

Understanding the basic functions of space technology, one may come to the most important conclusion on the purposefulness of their creation and enhancement. Although about three-quarters of artificial satellites that are launched into space are still executing the tasks of a military nature, it is cosmic systems that the critical infrastructure, including the military one, is dependent on at most. "Unpacking" elements of the infrastructure at the core of what technology enables its functioning is just simplifying the satellite and ground station.

In other words, satellite technologies as an asset or a resource which exists in suborbital space or cosmic space along with the ground control system, which includes the facilities to activate them. The space systems, in turn, belong to organizations that build, operate, maintain, service and own them. The examples of critical infrastructure and space systems interrelations exist in virtually every field of life. Agribusiness could not develop without a necessary system of weather and climate satellites, since the satellite remote sensing enables more immediate responses to natural disasters, better water, air and also soil moisture quality monitoring. Military potential would not exist without military and spy satellites. Economies of countries are based on the use of satellite navigation which is useful not only in giving time and position, but also in bank operations, in power distribution networks, telecommunications, dating measurements in automatic measuring instruments (probes, flowmeters, buoys, seismometers, etc.), and all types of transport (Fig. 1).

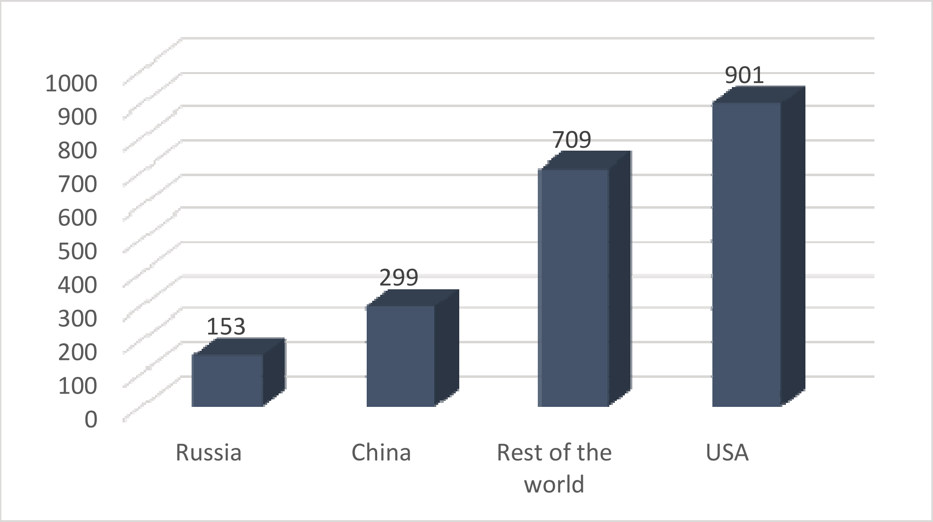

Fig. 1 The number of satellites in orbit on March 31, 2019 [7]

3 Cyberthreats

Apparently, space technology lags behind in the sphere of cybersecurity. The reasons for this are speculative in nature, however, using the example of the United States, one of the reasons may be a lower margin of space systems rather than the one obtained from defence systems or commercial activities. Moreover, certain security technologies (e.g. encryption) require more data processing power, while it is a valuable resource in space, and the priority in operation is other functionalities. Space systems are often developed “in the name of science” and technology developers do not even take into account the fact that their research project might become an attack target.

In order to properly secure any space mission, it is critical not only to understand its operation, but also to assess a number of the system vulnerabilities, which are also opportunities for hackers to be disrupted. This in turn requires a completely different knowledge in the area of security of the operational technology than the one which is common in the internal infrastructure of information technologies, including, among others, data management, servers and internal networks.

A lack of understanding of the discrepancies between the internal IT infrastructure and specialized space systems denotes that space systems are vulnerable to cyberthreats, and the specialists who have been assigned to tasks related to ensuring cybersecurity deal with a very wide range of IT issues. Moreover, the provision of cybersecurity means expenditures and highly skilled professionals. To make matters simple, quite often a system engineer is left alone with an issue of designing, implementing and checking cybersecurity tools, having only a limited time, resources, and knowledge to identify the defects in one's own project. Last but not least threat, at the organizational level, is an access of numerous stakeholders to sensitive information. Due to unique skills in the design and development of these systems and numerous sources required to complete the project, there is a necessity for fast and widespread sharing of various types of information, including the sensitive ones. NASA employees are constant targets of phishing attacks, which phish users' personal data, including, for example passwords [8-9]. If such an attack is successful, the undisclosed information can be used to easily attack a cosmic system. Such a risk enforces the need to analyse the standards of access to classified information and more stringent approach to the process of allocating information resources of this type. Digital attacks on space systems prove that even a highly subsidized project has got a number of shortcomings in the field of cybersecurity. Cyberattacks of space systems can be contractually divided into three groups:

- attacks on communication satellites,
- attacks on GPS systems, and
- attacks on government satellites and system architecture ground stations.

An example of the first type of cyberattack that used a satellite connection as a tool for Internet communication is the activity of the Russian cybercrime group Turla, which was analysed by the Russian antivirus software company – Kaspersky Lab in 2015. It turned out that the group that had been in operation for over eight years, conducted massive cyber-espionage, named by Kaspersky Lab experts – Epic Turla, infecting hundreds of computers in more than 45 countries, including Russia, China, the United States, and even Poland.

The targeted organizations included government institutions, embassies, as well as military, educational, research and pharmaceutical institutions. At the initial stage, the detrimental Epic software carried out victim profiling and eavesdropped transmissions from a satellite to identify active IP addresses of users who were online at that time. Having detected a high-level IP address, the attacker used it to disguise the C&C (command-and-control) servers. The hacker used the most common and affordable type of satellite Internet connection (the so-called downstream-only) through instructing the infected machines to transfer data to selected IP addresses that reached the satellites over traditional lines to the collective communication station of the Internet provider, next to the satellite and ultimately from the satellite to the selected users [10].

The vulnerability of the satellite communication mechanism consists in the fact that all transmission data come back to a computer in an unencrypted form, which allows its capture and access to all data collected by the users of these connections. It turns out that the necessary equipment costs less than $1 000. Command and Control (C&C servers) were the basis of sophisticated cyberattacks, at the same time being the weakest link in the detrimental infrastructure. The servers are readily analysed by law enforcement agencies of each country, as they can be used to track the physical location of the attackers. The Turla group hid their C&C servers through satellites, because their operations cover a large area and it is not possible to determine an exact place where the attacker is physically present. Turla used satellite Internet providers located in countries of the Middle East and Africa, such as Congo, Lebanon, Libya, Niger, Nigeria, Somalia and the United Arab Emirates [11-12] (Fig. 2). As a result, a hacker can be anywhere within the reach of a selected satellite, i.e. in an area exceeding thousands of square kilometres, making it virtually impossible to track them down. As rightly observed by the experts in the niebezpiecznik.pl website, all the attack techniques would almost be as perfect as Kaspersky wishes them to be, when describing them in their advertising materials if it had not been for the fact that eavesdropping someone else's satellite connection does not hamper tracking down perpetrators. It is rather a way to hamper tracking down the C&C server, which actually enables a prolonged attack [13]. Regardless of the extent of concealing cyberattacks on space systems, their effects can be more serious in the case of infection, e.g. an element of a critical infrastructure.

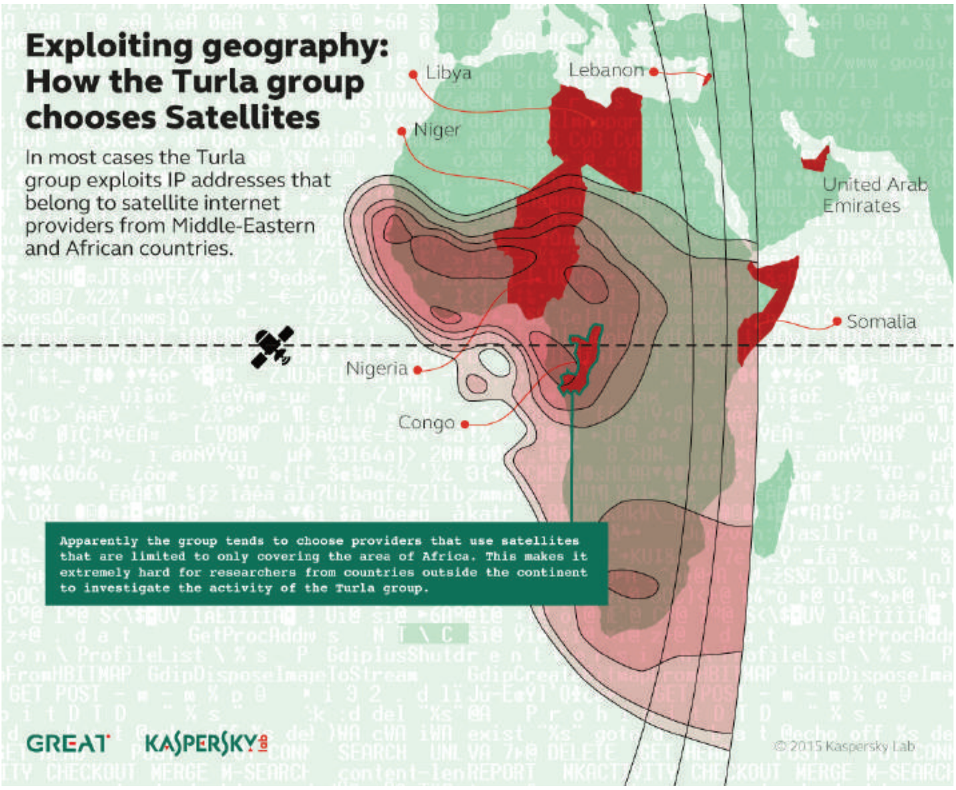
Exploiting geography: How the Turla group chooses Satellites
In most cases the Turla group exploits IP addresses that belong to satellite internet providers from Middle-Eastern and African countries.
Libya
Lebanon
Niger
United Arab Emirates
Somalia
Nigeria
Congo
Apparently the group tends to choose providers that use satellites that are limited to only covering the area of Africa. This makes it extremely hard for researchers from countries outside the continent to investigate the activity of the Turla group.
GREAT
KASPERSKY
© 2015 Kaspersky Lab

Fig. 2 Implementation of a satellite transmission by Turla Group [12]

The second group of cyberattacks in space systems is represented by attacks which are intended to disrupt or jam the GPS signal. Russia installed 250 000 jamming devices on civilian antennas around the country to disrupt the navigation of US missiles in case of a direct attack, although the American weapons, for example, Tomahawk missiles have got their own anti-jamming device to maintain their trajectory [14]. Although jamming a GPS signal is not treated as a cyberattack, spoofing a GPS signal is [15]. Moreover, it is more dangerous because it does not disrupt the operation, merely giving counterfeit data.

The subject of UAV interception, which relies much more strongly on the GPS than passenger aircraft, has been known for years. It is worth mentioning that military equipment uses an encrypted GPS signal, which is not susceptible to spoofing. Until now it has been common knowledge, however, that only Iran was successful in real-life combat conditions in 2011, when after jamming the communication channel, it "spoofed" a signal from the GPS satellite and sent a counterfeit data to a drone RQ-170 Sentinel (manufactured by Lockheed Martin) that its area of operation was Afghanistan. The US military claimed that the landing of the drone in Iran was a malfunction, however, they were unable to explain why the Iranians intercepted it intact [16].

One may try to alter the signal, which is sent to a satellite radio receiver, using the potential errors in the receiver so that the signal could cause a remote code execution. In this way, it is possible to establish unauthorized communication and make the satellite instruments execute a command on the basis of an unauthorized code. This kind of attack can escalate further systems. Such attacks would be difficult both to detect and to perform [17].

The third group of cyberattacks focuses on government satellites and ground-based elements of space systems. Public information about cases of such attacks is unfortunately abundant [18]. An example would be a double cyberattack in 2008 on the research satellite Terra EOS AM-1, which keeps observing the Earth for NASA, being a showcase of the Earth Observation System that consists of a series of satellites watching the Earth's surface, biosphere, atmosphere and oceans. In June 2008, hackers took control of the satellite for 2 minutes, and in October 2008 – for 9 minutes, however, they did not give the system any commands [19].

In view of all the above-mentioned vulnerabilities of the space sector as well as the strength and impact of cyberattacks, a question arises what steps need to be taken. The audit report for NASA in 2015 clearly indicates the need for reorganization and renewal of standards and cybersecurity protocols [20]. Private space company, i.e. SpaceX and Blue Origin, does not voice any comment on its general cybersecurity policy.

4 Problem Analysis

The 2001 report of the National Security Assessment Committee, referred to in the introduction, indicates that the importance of loss of a commercial satellite is incomparably lower than in the event of loss of a military or intelligence satellite. Especially in situations where the United States "works" to resolve international conflicts involving countries with nuclear potential, the loss of a military satellite adversely affects both a diplomatic and military advantage. The report also recalls the failure of computers in the ground station (in the early 2000), as a result of which the US lost all information from different satellites for three hours. Moreover, hackers routinely penetrated the network and computers of the US Department of Defence, and the number of attacks is growing due to an easier (then) access to hacking tools and techniques, which are becoming more and more sophisticated [21].

It also appears that aggressive actions against cosmic systems may often be confused with naturally occurring phenomena. Space junk and the Sun's activity could explain the loss of a system or mask a hostile action. However, the main reason is the failure of software or hardware, which in the end, may be the result of a hostile action.

The US government, industry and scientific environments make regular efforts to improve digital security of the critical infrastructure [22]. Yet, the attention paid strictly to the cyberspace of space systems is comparatively smaller. In 2013 the Aerospace Industries Association (AIA) published the first cybersecurity standards for space systems [23]. They particularly emphasize the cybersecurity of the manufacturers of these systems in the supply chain. It is unclear how they were actually adapted, because their implementation is voluntary and there is no mechanism for forcing their suppliers to introduce the standards under an existing contract. The material indicates that manufacturers and suppliers still face the problem of cybersecurity threats. Although IT network security has increased, the threat has not abated, because the attackers use the need for cooperation between different entities of the aerospace-defence sector, using suppliers as a “back door” [24]. Moreover, MITRE, a non-profit organization that manages governmental funds for research and development in the framework of public-private partnership, thus supporting several US government agencies, including the Department of Defence, has not yet published anything in the field of cybersecurity, dedicated to space systems, apart from a brief statement that the matter is crucial [25]. Space systems are much more complex than the systems of critical infrastructure, starting with issues related to their technological development and ending at the ownership and management issues. As a result, the digital protection of these systems still neither has its own guidelines in the form of standards, and nor any appropriate policies that might legalize these standards.

In fact, cybersecurity of space systems does not differ much from the industrial cybersecurity, however, its uniqueness contains several features that contribute to their weak points and vulnerability to attacks.

First, the cosmic system constitutes a Single Point of Failure (SPOF) for the critical infrastructure of various global economy and military activities sectors. To make it simpler, these are systems which, in the event of a failure, completely halt the operation of other associated systems [26]. As commonly known, the aim of a cyberattack is to maximize its effect with a minimal probability of detection. Therefore, from the perspective of a hacker, who wants to paralyze a commerce of a given country, targeting a satellite or multiple satellites operator, providing connection to the system of credit card terminals or inventory management is a rather easier way than disrupting the activities of e-commerce companies, i.e. the Amazon, attacking online payments, hacking or disrupting the activities of credit cards provider – Cardinal. Such corporations as Amazon or PayPal considerably invest in cybersecurity and constantly monitor their networks against fraudulent and malicious actions. Furthermore, the ability to influence several systems through breaching a single system intensifies the amount of vectors, in which a potential attack may be struck, both from the perspective of system architecture and a supply chain, because a given space system’s functioning depends upon the number of different individual components. In turn, each component of the system architecture is a potential attack vector. Fig. 3 depicts a simplified architecture of a simple space system.

Each of the components is primarily designed, manufactured, and serviced by another entity. Its digital advancement can vary considerably, and it is not always clear how much information, including that of dangerous nature, is shared by interrelated components. These issues are coupled with a variety of supply chains, controlled by the suppliers of all components, therefore, one minor flaw, malfunctioning, defect or an attack on any of these components may prove disastrous for the mission, causing incremental system failures.

The second feature of the space sector which affects the level of digital security space systems is the lack of space assets of cybersecurity standards, which would be regulated by any state at the national or governmental levels. Even if they existed, there would be no mechanisms of controlling their compliance. For this reason, it is highly probable that some satellites are used to conduct dangerous cyberoperations. It is particularly noticeable, from the point of view of the US experiences, that the equipment of the space system and communication components resistant to radiation or software requirements are extremely advanced and sophisticated. While the Federal Energy Regulatory Commission is responsible for the standards of electrical systems in the USA, and the International Telecommunication Union (ITU) is responsible for international regulations of satellites frequencies and also for the registration of their orbits, other standards are virtually non-existent [27]. Although in 2007, the ITU issued a report on global cybersecurity in order to introduce the "basic principles of international cooperation on cybersecurity," it seems that since then the issue has not been updated by the ITU, despite the rapidly changing environment of cybersecurity [28].

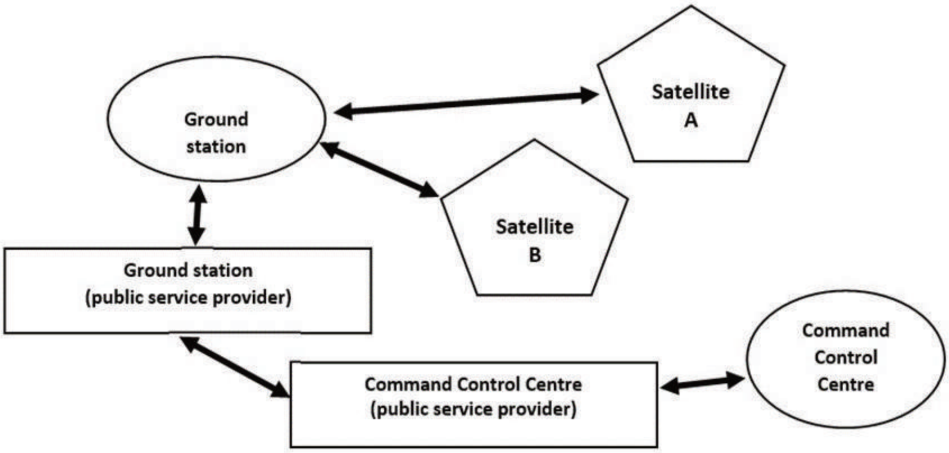
Ground station
Satellite A
Satellite B
Ground station (public service provider)
Command Control Centre (public service provider)
Command Control Centre

Fig. 3 Space system architecture

Another (third) characteristic feature of the space sector is a particularly complex supply chain of products, services, and a product life cycle. From the perspective of a hacker, interdependence among suppliers of various components for space systems is a conducive condition, especially as the situation in which there is only one system manufacturer or a supplier of all parts is extremely rare. Several manufacturers of various technological specializations develop their own different technologies, and yet another entity is the final integrator of these technologies. A good example might be the Polish company Creotech Instruments S.A., which as a subcontractor of the Space Research Centre at the Polish Academy of Sciences, built an experimental system of conversion and power distribution, developed for the ASIM (Atmosphere-Space Interactions Monitor) device, launched into the Earth's orbit in 2018 by a Falcon-9 rocket manufactured by the SpaceX company [29]. Besides, in accordance with a report issued by the Polish Space Agency in 2017, the use of satellite data, in the years 2013-2016, constituted as much as 35 per cent of all the contracts received by Polish entities from the European Space Agency. Exploiting satellite data is a dominant scope of interest and experience of Polish entities, since their implementation does not require the initial technological facilities. Other areas of technology can sometimes become technological niches, in which Polish entities have a chance to enter the supply chain [30] (Fig. 4).

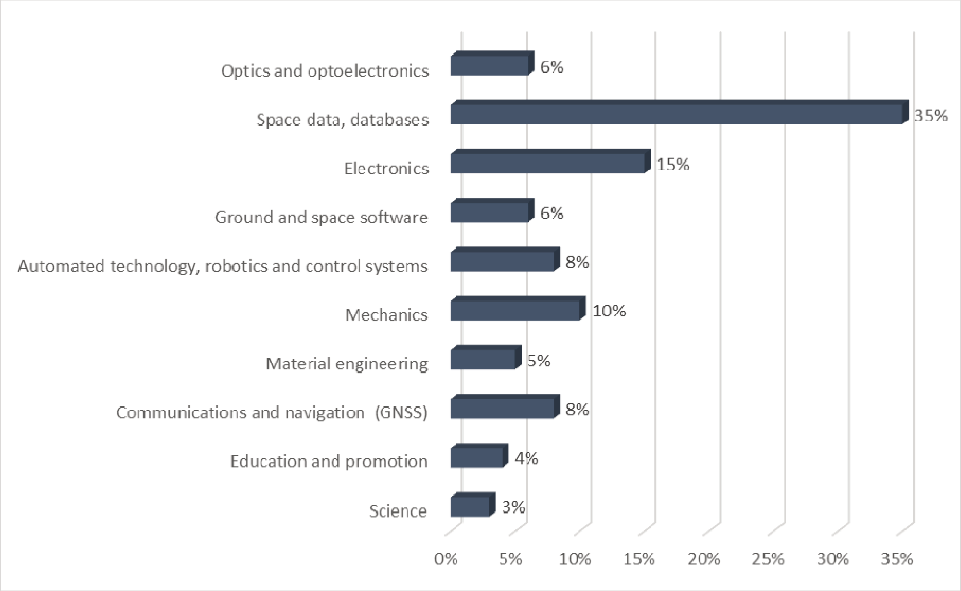

Fig. 4 Technological areas designated under contracts received by Polish entities from the European Space Agency in the years 2013-2016 [30]

In order to reduce the costs, even National Aeronautics and Space Administration (NASA) purchases components of space systems from “ready-made” catalogues of approved suppliers from around the world [31]. Each successive supplier provides an opportunity for a hacker to implement a digital threat to the entire system. An additional risk is a scenario in which a government agency, e.g. NASA, when purchasing a part from a supplier, has no control who has designed a printed board, intended for mounting electronic components, or who wrote a source code for a given component.

Moreover, this extremely complex supply chain makes it impossible to identify an entity which is held responsible for operations and finances for ensuring cybersecurity since, unlike the majority of entities in the sector of critical infrastructure, the organizations that manage the infrastructure of space systems, are not their owners. The discussed product life cycle is complex also due to the plurality of stakeholders involved in its development. Its “viability”, understood as a period of operation, must be substantial. Space missions can continue over decades. Therefore, the threat to the digital system is growing. At the time of its launching, the system was probably sufficiently protected, however with time its protection may prove insufficient. The diagram below shows the risks and responsibilities for a sample satellite project in the USA [32] (Fig. 5).

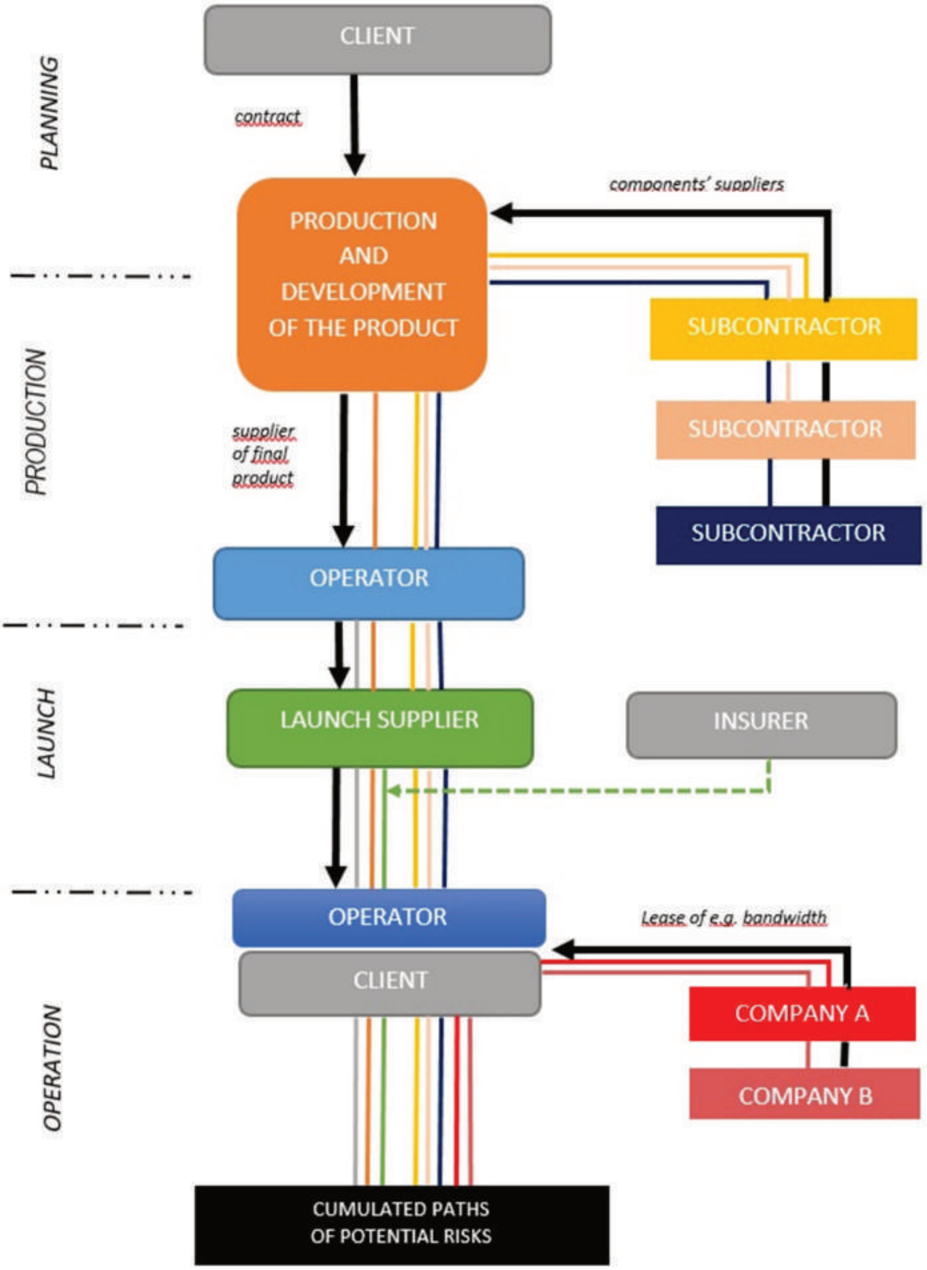

Fig. 5 Threats and responsibilities for a sample satellite project [32]

As in the case of industrial control systems of critical infrastructure, space systems, especially those which are critical, are built in order to operate over a long period of time and with no possible stoppage. This makes them particularly vulnerable to threats. Even if non-existent now, they may be devised by hackers in the future. The fourth feature of the space sector is a common phenomenon of using commercial software – the so-called “off-the-shelf”, which is available immediately. Not all satellites are as complex as those that have strict security protocols. The miniature, low-cost satellites (CubeSat), which at the launch time have a mass of approximately 1 kilogram, and an option of multiplying their size, from a technological point of view, have a relatively low entry barrier, commercially using mass-produced, ready for sale software versions, referred to as (Commercial-Off-The-Shelf – COTS), which are sold to the customer without being adapted to their needs, and consequently being cheaper [33]. Although their typical use is education, observation and research, and they were designed by an institution with an appropriate budget, it is not excluded that any larger company or a wealthy person may have such a budget (approx. 100 000 USD). The first threat type of using COTS products is a scenario in which users do not maintain or update, even if necessary, these systems in terms of security. Secondly, the contribution to the design or programming a code can be made by anyone, which means that the system vulnerability may be intentionally implemented by the enemy in the system code. In 2017 years, roughly 700 miniature artificial satellites were estimated to remain in orbit [34]. Their use by public and private entities results in an increase in their vulnerability of the ecosystem of information technology, as long as the micro-satellites are not properly secured (government agencies tend to lease the selected bands of commercial satellites) [35]. Hacking micro-satellites which have their own propulsion system and bringing them to a collision with another satellite seems quite feasible. Although, for the time being, satellite collisions are accidents, the intentional actions can be devastating [36].

5 Conclusions

Space systems enable the vast majority of critical infrastructure in the world to operate. The scientific, political and industrial communities understand the relevance of critical infrastructure cybersecurity, although space systems are regarded as a domain which remains beyond this area. Today, however, it is clear that space systems are the weakest link in the critical infrastructure systems.

Entities of the space sector need not idly wait for political decisions, because there are areas of action that can be implemented almost instantly. In the first place, there are certain cybersecurity standards in the United States and therefore, it is essential to implement them in the process of security design and development. The good examples might be cybersecurity standards developed by the National Institute of Standards and Technology (NIST), which as a federal agency has an analogous role to the Polish Central Office of Measures [37]. Obviously, some standards may not be applied to specific space systems. However it should automatically initiate the process of designing, testing and demonstration of new standards, appropriate for the specific and unique system. Moreover, all stakeholders of space systems should be involved in the process of adapting these standards, including the need to prove their use by each and every subcontractor.

Bearing in mind the fact that operational and information technologies have different operational requirements and with regard to digital protection, it is essential to take into account the delegation of competences and skills among specialists in the field of cybersecurity of space systems and those responsible for internal security systems.

It should also be mentioned that an allocation of specific resources in order to counteract or minimize the risks of digital threats should be definitely included in the budgets of space missions. Moreover, there is a question of the introduction of risk assessment in the field of cybersecurity for each mission, and an intensive cooperation with research centres, which are associated with the security of information and operational systems.

Finally, based on the international will to share experience and knowledge of risk assessment and various responses to threats, the international space regime with all cybersecurity stakeholders has the best chance to develop solutions for the whole space sector, because only in this way it is possible to match the currently available and planned solutions to such an extremely wide spectrum of threats to space systems.

References

[1] MYSZONA-KOSTRZEWA, K. Satellite Navigation in the Light of International Law and the European Union (in Polish). In: Z. GALICKI, T. KAMIŃSKI, K. MYSZONA-KOSTRZEWA, ed. *The Use of Space. World-Europe-Poland*. Warsaw: Sawpiauw, 2010. ISBN 978-83-927864-6-7.

[2] *U.S. Military Preparing for a War without GPS* [online]. December 2017 [viewed 2019-09-01]. Available from: https://www.straitstimes.com/world/united-states/us-military-preparing-for-a-war-without-gps

[3] SMITH, M. *Trump National Security Strategy Promotes, Protects Space* [online]. December 2017. [viewed 2019-09-01]. Available from: https://spacepolicyonline.com/news/trump-national-security-strategy-promotes-protects-space/

[4] *Report of the Commission to Assess United States National Security Space Management and Organization* [online]. January 2001. [viewed 2019-08-30]. Available from: https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf

[5] MYSZONA-KOSTRZEWA, K. Satellite Techniques and Security and Defense (in Polish). In: *Legal Aspects of Space Activities*. Warsaw: Redakcja naukowa, 2019. ISBN 978-83-65711-53-2.

[6] *Satellite Technology* [online]. [viewed 2019-12-01]. Available from: https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/satellite-technology

[7] *Number of Satellites in Orbit* [online]. [viewed 2019-12-06]. Available from: https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/

[8] KORTEPETER, D. *It's not Rocket Science: NASA Unit Hobbled by Amateurish Phishing Attack* [online]. June 2019. [viewed 2019-09-05]. Available from: http://techgenix.com/nasa-jpl-phishing-attack/

[9] *What Is Phishing?* (in Polish) [online]. [viewed 2019-09-04]. Available from: https://www.securelist.pl/threats/internal/7058, co_to_jest_phishing.html

[10] *Turla, a Cybercriminal Group, Uses Satellites to Achieve Anonymity* (in Polish) [online]. September 2015. [viewed 2019-09-07]. Available from: https://www.kaspersky.pl/o-nas/informacje-prasowe/2485/ugrupowanie-cyberprzestepcze-turla-wykorzystuje-satelity-w-celu-osiagniecia-anonimowosci

[11] *Russian-Speaking Cyber Spies Use Satellites)* (in Polish) [online]. [viewed 2019-09-07]. Available from: https://plblog.kaspersky.com/?s=Rosyjskoj

%C4%99zyczni+Cyberszpiedzy+Wykorzystuj%C4%85+Satelity+[12]*Satellite Turla: Still Alive and Hiding in the Sky* [online]. [viewed 2019-09-07]. Available from: https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf

[13] *The Russians Are Attacking Satellite Connections to Stay Anonymous Online* (in Polish) [online]. September 2015. [viewed 2019-09-06]. Available from: https://niebezpiecznik.pl/post/rosjanie-atakuja-satelity-aby-zachowac-anonimowosc-w-sieci/

[14] DALTON, A. *Russia Hopes to Block Cruise Missile Attacks with Cell Towers* [online]. October 2016. [viewed 2019-09-08]. Available from: https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/

[15] *The Sensitivity of the GPS Satellite Navigation System to Interference* (in Polish) [online]. November 2019. [viewed 2019-09-08]. Available from: http://www.filambda.amw.gdynia.pl/2016/11/29/wrazliwosc-systemu-nawigacji-satelitarnej-gps-na-zaklocenia/

[16] *Iran Intercepted an American Spy Plane* (in Polish) [online]. December 2011. [viewed 2019-09-15]. Available from: https://niebezpiecznik.pl/post/iran-przechwycil-amerykanski-samolot-szpiegowski/

[17] ZIEMNICKI, P. *The Fundamental Importance of Securing Satellites against Cyber Attacks* (in Polish) [online]. February 2019. [viewed 2019-09-13]. Available from: https://www.space24.pl/analizy/fundamentalne-znaczenie-zabezpieczenia-satelitow-przed-cyberatakami-wywiad

[18] BYRNE, D., D. MORGAN, K. TAN, B. JOHNSON and C. DORROS. Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations. *Procedia Computer Science*, 2014, **28**, pp. 522-530. DOI 10.1016/j.procs.2014.03.064.

[19] *U.S.-China Economic and Security Review Commission* [online]. November 2011. [viewed 2019-09-15]. Available from: https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

[20] *NASA's Management of the Deep Space Network* [online]. March 2015. [viewed 2019-09-16]. Available from: https://oig.nasa.gov/docs/IG-15-013.pdf

[21] *Commission to Assess United States National Security Space Management and Organization* [online]. January 2001. [viewed 2019-08-30]. Available from: https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf

[22] *Improving Critical Infrastructure Cybersecurity* [online]. [viewed 2019-08-28]. Available from: https://www.dhs.gov/sites/default/files/publications/cisa_-_improving_critical_infrastructure_cybersecurity.pdf

[23] *AIA Announces First Cybersecurity Standard* [online]. February 2013. [viewed 2020-02-28]. Available from: https://www.aia-aerospace.org/news/aia-announces-first-cyber-security-standard/

[24] KING M. and S. GOGUICHVILI. *Cybersecurity Threats in Space: A Roadmap for* Future *Policy* [online]. [viewed 2021-04-05]. Available from: https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy

[25] *Securing Civil Space* [online]. [viewed 2019-08-26]. Available from: https://www.mitre.org/capabilities/cybersecurity/securing-civil-space

[26] *Securing Civil Space* [online]. [viewed 2019-09-01]. Available from: https://www.mitre.org/capabilities/cybersecurity/securing-civil-space

[27] *What FERC Does* [online]. [viewed 2019-09-01]. Available from: https://www.ferc.gov/about/what-ferc/what-ferc-does

[28] *ITU Global Cybersecurity Agenda (CGA)* [online]. International Telecommunication Union, 2007. [viewed 2019-09-02]. Available from: https://www.itu.int/osg/spuold/cybersecurity/gca/docs/global-cybersecurity-agenda-itu-17-may-2007.pdf

[29] *On Monday, the Launch of a Space Mission with Polish Participation* (in Polish) [online]. March 2018. [viewed 2019-09-02]. Available from: http://naukawpolsce.pap.pl/aktualności/news%2C28912%2Cw-poniedzialek-start-kosmicznej-misji-z-polskim-udzialem.html

[30] *Polish Space Sector Catalogue of Selected Entities* [online]. Warsaw: Polish Space Agency, 2018 [viewed 2021-03-26]. ISBN 978-83-64423-80-0. Available from: https://polsa.gov.pl/images/polski_sektor_kosmiczny_katalog_pl_eng/PODGLAD_PAK-KATALOG_EN_small.pdf

[31] *NASA Parts Selection List (NPSL)* [online]. February 2016. [viewed 2019-09-02]. Available from: https://nepp.nasa.gov/npsl/

[32] FALCO, G. *Job One for Space Force: Space Asset Cybersecurity* [online]. Cambridge: Belfer Center for Science and International Affairs, 2018 [viewed 2019-07-26]. Available from: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf

[33] *CubeSat Launch Initiative* [online]. [viewed 2019-09-03]. Available from: https://www.nasa.gov/directorates/heo/home/CubeSats_initiative

[34] DAVID, L. *Sweating the Small Stuff: CubeSats Swarm Earth Orbit* [online]. July 2017. [viewed 2019-09-03]. Available from: https://www. scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit/

[35] SCHRADIN, R. *Government Space Leaders Look to Commercial Satellites for More Resilient Communications* [online]. January 2016. [viewed 2019-09-03]. Available from: https://ses-gs.com/govsat/defense-intelligence/government-space-leaders-look-to-commercial-satellites-for-more-resilient-communications/

[36] PULTAROVA, T. *Could Cubesats Trigger a Space Junk Apocalypse?* [online]. April 2017. [viewed 2019-09-03]. Available from: https://www.space.com/36506-cubesats-space-junk-apocalypse.html

[37] CIESLAK, N. *NIST Cybersecurity Framework Adoption on the Rise* [online]. March 2016. [viewed 2019-09-20]. Available from: https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise