Teka Kom. Praw. – OL PAN, t. XI, 2018, nr 2, 329–346

SAFETY AND SECURITY LAW: SPACE SITUATIONAL AWARENESS SYSTEM (SSA) IN TRANSATLANTIC RELATIONS. EUROPE VIS A VIS THE US

Małgorzata Polkowska

Department of Administration and International Law
War Studies University
Poland
https://orcid.org/0000-0002-6633-2222

Summary. This article undertakes a very sensitive issue such as space security and its implementation urgency into national law. There are a number of challenges to the security of space infrastructure, such as unintentional threats (space debris), intentional threats (space weapons, malicious interference, cyber-attacks) or threats related to the weather in space (geomagnetic storms, solar storms, etc.) Space is increasingly congested and various prevention and protection measures need to be implemented. On the other hand, there is a growing dependence on the space of some countries, including European ones. There is therefore an urgent need to speed up this work on security and international cooperation, e.g. between the European Union and the US – the "space leader". The transatlantic cooperation between European states and the US is crucial in the area or space security. The US has necessary knowledge in its long history of experience of making space strategy, policy and security law and may be a good example for Europe in building the safety and security structures in space.

Key words: space security, space security awareness, security law, space strategy

INTRODUCTION

This article undertakes a very sensitive issue such as space security and its implementation urgency into national law. The transatlantic cooperation between European states and the US is crucial in this area. The US has necessary knowledge in its long history of experience of making space strategy, policy and security law[1].

[1] M. Polkowska, *Prawo bezpieczeństwa w Kosmosie*, Instytut Wydawniczy EuroPrawo, Warszawa 2018, pp. 15–27.

THE SPACE SECURITY

Space Security is defined by the Space Security Index as “the secure and sustainable access to, and use of, space and freedom from space-based threats”. This definition encompasses the security of the unique outer space environment, which includes the physical and operational integrity of man-made assets in space and their ground stations, as well as security on Earth from threats originating in space. This definition can be expanded further to encompass the crucial role played by space systems in support of defense and security activities on Earth. In this report, ‘Space Security’ is understood primarily as ‘Security in Outer Space’ referring to the protection of space infrastructure from threats so that this infrastructure can fulfil its specific functions as expected. In this case, activities in the field of Space Security encompass the set of political, legal, economic and technical provisions required to ensure an “accessible”, “affordable” and ”safe to operate” in space environment. There are three definitions “security in Outer Space” (the protection of the space infra-structure against natural and man-made threats or risks, ensuring the sustainability of space activities and “Outer Space for Security” (the use of space systems for security and defense purposes. “Security from Outer Space” means the protection of human life and the Earth environment against natural threats and risks coming from space.

The space infrastructure can be described as a network of space-based and ground-based systems interconnected by communication channels and enabled by access to space capabilities. It includes: a space segment (all systems of the infrastructure located in orbit, namely satellites required for the conduct of operations and delivery of intended service), a ground segment (all systems of the infrastructure located on the surface of the Earth and necessary for the conduct of operations in space and delivery of data and signals), an user segment (sub-part of the ground segment and composed of complementary ground-based systems required for the delivery of full-fledged space services accessible by end-users) and a down-links and up-links to interface between the space and ground segments (i.e. including users’ equipment) and to operate the space system and receive its data. The uplink refers to signals trans-mitted from the ground to space and the downlink refers to signals received on the ground from space[2].

[2] ESPI (European Space Policy Institute), Vienna, report June 2018 Security in Outer Space: *Rising Stakes for Europe*, report 64.

In the 21st Century while mentioning the space we should put attention into three “c” – congested, contested and competitive as a scene for implementation of space law regulations.

1. The Congested Space

From the beginning of the Space Age and the first satellite launch, i.e. Sputnik-1 on the 4th of October 1957 the number of space debris exceeds the number of operational satellites. As such space debris poses a threat to the Near Earth environment on the Global scale[3]. The first awareness of the problem came out in 1960s, based on the research activities undertaken in the US. In 1978 Donald Kessler[4] concluded that the generation of space debris via collision and in-orbit fragmentations may lead to an exponential increase in the amount of the artificial objects in Space what would render spaceflight too hazardous to conduct.

Currently, the total number of the objects larger than 10 cm reached the number more than 17 000 objects and object between 1cm and 10 cm approx. 500 000 among which only approx. 1400 are active satellites. Those remnants of human activity around space encompass all the inactive, manmade objects, including the fragments that are orbiting Earth or re-entering the atmosphere. The majority of catalogued object however originated from more than 290 break-ups in orbit, mainly caused by the explosion, and from about 10 suspected collisions (of which four are confirmed between the catalogue objects). That debris creates the significant risk to the Space infrastructure as the collision with debris larger than 1 cm could disable an operational satellite or could cause the break-up of a satellite or the rocket body. Moreover, the impact by the debris larger than about 10 cm can lead to a catastrophic break-up as complete destruction of a spacecraft and generation of a debris cloud.

The major contributions to the population of the fragments came from a Chinese Anti-Satellite test targeting the Feng Yun-1C Weather Satellite on 11 January 2007, which created more than 3400 tracked fragments, and the approximately 2300 tracked fragments created from the first ever accidental

[3] *The status and future evolution of Transparency and Confidence Building Measures*, in: *The prospects for Transparency and Confidence-Building Measures in Space*, eds. J. Robinson, M.P Schaefer, K-U. Schrögl [et al.], ESPI Report 27, Vienna 2010.

[4] B.G. Cour–Palais, D.J. Kessler, *Collision frequency of artificial satellites: The creation of a debris belt*, “Journal of Geophysical Research” 83 (1978), issue A6, pp. 2637–2646.

collision between two satellites, Iridium-33 and Cosmos-2251 on 10 February 2009.

Many years of technical discussion and various exchanges reflected in the leading body in the field of space debris i.e. Inter-Agency Space Debris Coordination Committee (IADC) founded in 1993 by ESA, NASA, Japan Space Agency (JAXA) and Russian Space Agency (ROSCOSMOS) (complemented by the other space agencies later on). The significance of those issues has been recognized globally and some measures where applied as the nearly universal adoption of the Liability Convention[5] IADC's Space Debris Mitigation Guidelines[6] or some work being performed at the level of the Technical Subcommittee of the United Nations' Committee on the Peaceful Uses of Outer Space (UN COPUOS) since 1994. However, the standardization measures are required in order to achieve a common understanding of the require task leading to the transparent and comparable processes as works performed with ISO.WD 24113 Space Debris Mitigation[7]. Additionally in order to address the issues posed by the Space debris on spacecraft activities UN COPUOS has taken the initiative to create a set of internationally agreed Guidelines for the long-term sustainability of outer space activities[8].

The growing number of the spacecraft deployed around the Globe and the growing trend of their miniaturization significantly multiplies the risk of in-orbit collision[9]. Due to that fact, the systematically grows caused the necessity to gather more precise information on the location of the Earth orbiting objects. Moreover, all expert analyses highlight the risk collision which will increase significantly with appearance of so called mega-constellations (hundreds to thousands of Satellites).

This trend has been noticed worldwide and as such reflected as global concern within the international fora.

---

[5] United Nations, Convention on International Liability for Damage Caused by Space Objects 1972.

[6] IADC (Inter-Agency Space Debris Coordination Committee), Space Debris Mitigation Guidelines 2002.

[7] ISO (International Standard Organization), Space Systems – Space Debris Mitigation, ISO TC 20/SC 14, 2011.

[8] United Nations, Guidelines for the long-term sustainability of outer space activities, A/AC.105/L.315, 2018.

[9] J. Radtke, Ch. Kebschull, E. Stoll, *Interactions of the space debris environment with mega constellations – Using the example of the OneWeb constellation*, "Acta Astronautica" 131 (2017), pp. 55–58.

2. The Contested Space

Beside the space debris, there are other challenges the contemporary space must face to. The today's world is the more and more dependent on the space assets and in parallel there is more and more countries able to perform hostile actions against the space related infrastructure (ground-based and space-based)[10]. These issues are both related to the civil security and the defense, of course. In civil world the fast growing dependence on usage of assets as Global Navigation Satellite Systems (GNSS such as GPS and Galileo) or strong dependence its easy visible. Lack of access to the space-based systems or disruption in the continuity of the services may significantly shake the economy of the countries and its internal security. This is even more visible in the military domain where the recent wars in Afghanistan and earlier in Iraq revealed universality of the space assets in the contemporary wars. Those wars were the first real space wars with the wide scope of the space assets utilized. The modern spaced systems like information gathering satellites were vastly used by performing missions contributing to the mission preparation, execution and the effects assessment. The similar situation concerns other asset as GNSS Guidance Munition and Satellite Communications.

However, other countries like Russia, China or India recognize the dependence of the NATO and the US on space assets[11]. Because of it they pursue to develop counter-space capabilities like Anti-satellite weapon, electronic warfare, cyber and jamming capabilities, laser disabling or rendezvous and proximity operations (RPO).

The NATO and the national answer to the developing of counter-space activities by hostile states imposed the urgent need to improve SSA capabilities[12]. In particular, the US signed so-called SSA Data Sharing Agreements and cooperating in military SSA exercise as the Global Sentinel.

[10] A.A Faiyetole, *Potentialities of Space-based Systems for Monitoring Climate, Policies and Mitigation at Climate Policies and Mitigations of Climate Process Drivers*, "The International Journal of Space Politics and Policy" 14 (2018), no. 8, pp. 28–48; SWF (Space World Foundation), *Global Counter space Capabilities: An Open Source Assessment*, April 2018.

[11] S. Paracha, *Military dimensions of the Indian Space Programs*, "The International Journal of Space Politics and Policy" 11 (2013), no. 3, pp. 156–186.

[12] J.J. Klein, *The influence of Technology on Space Strategy*, "The International Journal of Space Politics and Policy" 10 (2012), no. 1, pp. 8–26.

3. The Competitive Space

At the beginning of the 21st century the International community is witnessing the confluence of the several powerful economic and the policy forces in the Global space sector[13]. Due to the financial constraints at the governmental level, the emergence of a new space markets and involvement of the venture capital in the commercialization of space market are increasing rapidly. In the same time the technology dissemination and lowering of the entrance level are bringing the new opportunities to the public space programs, introducing some New Space Actors.

Moreover, this change of commercial space is being performed within the world also experiencing the number of changes that are rapidly and vastly reshaping the global context, making in more complex and challenging. Five major global trends are dominant to the Horizon 2030:

a) the globalization will continue moving towards more interdependence, but also fragmented governance and insecurity (in particular as regards the cyber- insecurity);

b) the revolution in the technologies and their application will continue to transform the societies in almost every aspect;

c) the nexus of climate change, energy and resources (including food security and water supply) will intensify;

d) the shift in the world economy towards Asia will continue;

e) the ageing will be global; Europe will be the "oldest" region; inequalities (in different forms, e.g. income, age, gender, digital divide …) will persist; and migration may well further increase[14].

In this environment the key driver of the Space change[15] today is the enabling of major change in the commercial launch and satellite manufacturing industries. While relatively small markets today, rapidly falling costs are lowering the barrier to participate in the Space economy, making new industries like a space tourism, asteroid mining, and on-orbit manufacturing viable, and growing existing flagship communications satellite services busi-

---

[13] C. Al–Ekabi, S. Feretti, *Yearbook on Space Policy 2016 – Space for sustainable development*, ESPI, Vienna 2018, p. 1 and following.

[14] European Strategy and Policy Analysis System (ESPAS), *Global Trends to 2030: Can the EU meet the Challenges Ahead?*, 2015; World Economic Forum, Global Risks Report 2017, 12th Edition, Geneva 2017.

[15] *Profiles in Innovation: Space: Next Investment Frontier*, Goldman, Sachs & Co., April 2017.

ness while taking exploration deeper into space. Space is also becoming a military focal point as government pivot off Earth.

All above trends in Space (i.e. increased number of space objects, militarization and commercialization)[16] make the space much more busiest place that must be appropriately reflected in effective SSA and its evolution and bifurcation to Space Traffic Management. Additional supplementing operational aspects as SWE and NEO both enhance maturity and effectiveness of SSA system and protection and security in space and on the ground.

INTERNATIONAL COOPERATION IN SPACE

International partnerships on space security have their roots in the Second World War, when sensitive information was marked "Eyes Only" for the nationalities of the "eyes" that could have access to specific sorts of information. Today, five World War II allies – United States, Australia, Canada, New Zealand and the United Kingdom – continue to participate in a range of important and interrelated security cooperation arrangements. During World War II, crucial and enduring partnerships were forged between the United States, Canada and the United Kingdom in the Battle of the Atlantic and during the liberation of Western Europe. Similar close and enduring cooperation also took place in the Pacific with Australia and New Zealand. While some dwell on the role of "Ultra" or "Magic" intelligence, it's important to recall that the Allied victories were due to a combination of a range of Failing this, dependence on third countries would persist even though there would be a shift from direct dependence on foreign space systems (e.g. GPS) to dependence on foreign capabilities to secure European systems[17].

Space cooperation can take many forms, such as multilateral cooperation at the international or regional level and bilateral cooperation with individual countries. Depending on the format of this cooperation, countries may designate specific agencies or institutions as the main representative, but the acti-

[16] R.G. Harrison, *Unpacking the Three C's: congested, competitive and contested Space*, "The International Journal of Space Politics and Policy" 11 (2013), no. 3, pp. 121–131.

[17] Remarks of R.H. Buenneke, *Senior Advisor, National Security Space Policy Office of Emerging Security Challenges Bureau of Arms Control, Verification and Compliance U.S. Department of State Panel on "Balancing national security and economic security in a contested and congested space domain" "Greater Security Through International Space Collaboration" Seminar George Washington University Space Policy Institute The Aerospace Corporation's Center for Space Policy & Strategy*, July 19, 2018, pp. 1–5.

vity may involve other agencies or departments and non-governmental representatives from industry or academia. At the multilateral level, active participation in the key space forums (e.g., the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), International Telecommunication Union (ITU), as well as related forums for cooperation in specific application areas (e.g., the Group on Earth Observations for cooperation in Earth observation), is often considered a fundamental aspect of these activities. Countries see it as both a way to exert leadership and ensure their views are represented in relevant exchanges at the international level and a way to share information about their space activities and learn of the activities of others.

This participation may thus influence policy debates at the national level. At a regional or bilateral level, countries may adopt multiple mechanisms to formalize relationships – whether issuing joint declarations or statements, signing cooperative agreements to pursue specific activities together or to exchange data, pooling institutional or financial resources in a cooperative program, or other methods. Regional space cooperation organizations have also emerged as a way to improve cooperation in and coordination of space activities at the regional level. For example, the Asia-Pacific Regional Space Agency Forum (APRSAF) seeks to advance space activities in the Asia-Pacific region with institutions from more than 40 countries participating.

Governments occupy a range of roles in their interaction with the private sector: regulator, customer, supplier (of technology and intellectual property), collaborator, and competitor. The way these roles are expressed is a major influence on the development of a broader space industry outside of the government program in a given country. Along with its role in the market as a regulator, government also exerts considerable influence through its role as a customer. Governments must be aware of how the choices they make in engaging the private sector through the procurement of goods and services affects both the development of industry and the evolution of government space strategy and programs[18].

[18] M. Othman, *National Space Policy and Administration*, in: *Handbook for New Actors in Space*, ed. C.D. Johnson, Secure World Foundation, 2017, pp. 54–87.

SPACE SECURITY CHALLENGES

The space domain is undergoing a significant set of changes. A growing number of states and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth, but also more congestion and competition in space. From a security perspective, an increasing number of states are looking to use space to enhance their military capabilities and national security. The growing use of, and reliance on, space for national security has also led more states to look at developing their own counterspace capabilities that can be used to deceive, disrupt, deny, degrade, or destroy space systems.

The existence of counterspace capabilities is not new, but the circumstances surrounding them are. Today there are increased incentives for development, and potential use, of offensive counterspace capabilities. There are also greater potential consequences from their widespread use that could have global repercussions well beyond the military, as huge parts of the global economy and society are increasing reliant on space applications. There is a significant development of a broad range of kinetic (i.e. destructive) and non-kinetic counterspace capabilities in multiple states. However, only non-kinetic capabilities are actively being used in current military operations.

Space Weather

"Space weather" is the term for the set of physical and electromagnetic processes and effects that occur on the sun, and ultimately interact with the Earth's magnetic sphere, atmosphere, and surface. These phenomena, which include solar flares, solar wind, geomagnetic storms, and coronal mass ejections, can have adverse effects on activities in orbit and on the Earth's surface. The sun is constantly emitting electrically charged particles, which flow outward throughout the solar system in a phenomenon known as solar wind. The sun also emits electromagnetic radiation across a variety of wavelengths including radio, infrared, visible light, ultraviolet, and X-rays. Changes in the intensity of these emissions result in the variety of effects known as space weather events, including: sunspots, which can lead to increased emission of solar wind, coronal mass ejections, which correlate with increased numbers of electrically charged particles being ejected into the solar wind, and which have effects similar to those of sunspots, coronal holes, which also cause increased solar wind activity, solar flares, which result in high-concentration bursts of radiation.

Outside of the aurorae, space weather affects are generally not visible to the naked eye. For the most part, the Earth's natural magnetic field protects the planet from the general solar and radiation environment. However, when space weather events occur, they can have deleterious impacts on spacecraft operations that operators need to be aware of. These include: higher levels than normal of charged particles, which might degrade satellite components and equipment; interference with electrical signals, including those of high-frequency and ultra-high-frequency communications satellites and global navigation satellite systems (GNSS), interference with radar and/or space tracking systems looking in sunward or poleward directions, increased drag for satellites operating in low Earth orbit; and the potential for increased radiation exposure for humans in orbit.

Strong space weather events can also impact vulnerable systems on Earth's surface, including electrical power grids and aviation systems. Space weather is typically correlated with an 11-year cycle of solar maximum and minimum, although notable events can occur at any point in the cycle. Government agencies, including the National Oceanic and Atmospheric Administration's Space Weather Prediction Center (NOAA SWPC) and the US Air Force, provide space weather forecast services, including offering watches, warnings, and alerts. Depending on the type of space weather event, warnings, watches, and alerts can be issued with between 10 minutes and 72 hours of advance notice. Space weather events are rated by a published scale to describe their expected severity. Operators and other interested parties can subscribe to the forecast service via NOAA's Space Weather Prediction Center[19].

A hybrid space operation

A common characteristic of hybrid space operations is that they often involve ambiguous attribution, temporary and reversible effects, and are generally not visible publicly. Space is, by nature, a critical domain for hybrid operations and warfare. In that sense, it is no different from land, air, sea, and cyberspace. NATO, as a military alliance dependent on space assets (e.g. SATCOM, ISR, integrated tactical warning and attack assessment, weather information, Position, Navigation and Timing, etc.), is exposed to space related threats. NATO is aware that the maintenance and security of space-based

[19] G. Wyler, *Responsible Operations in Space*, in: *Handbook for New Actors in Space*, pp. 118–119.

systems are critical for the Alliance. Accordingly, it acknowledges the importance of SSA, which it defines as "the knowledge and the understanding of military and non-military events, activities, circumstances and conditions within and associated with the space environment or space-related systems that are relevant for current and future NATO interest, operations and exercises". Any effort aimed at developing effective multinational SST networks to enhance SSA, like the European SST project, is welcomed by NATO.

A number of activities dealing directly or indirectly with space hybrid operations are now underway in Europe. To accelerate this positive momentum, consideration should be given to the following recommendations: elevate further the visibility of space hybrid operations so that this rapidly evolving threat indecisively taken off of "back-burner" status; work to identify capability gaps, including the tracking and mapping of space incidents and the quick ability to differentiate between anomalies and space hybrid operations; organize regular meetings of space security officials and experts to discuss the latest developments in this threat environment; organize tabletop exercises and simulations to rehearse the operational aspects of detecting, attributing, characterizing and reacting to space hybrid incidents; educate and train personnel in operations centers concerning these threats, including the E&F "space sector capture" predations of China and Russia globally; review classification standards related to these threats to enable partner and allied access to essential information; include these threats in the development of a Space Domain Awareness (SDA) architecture; consider cross-domain deterrence or response options in the E&F space by putting at risk continued unfettered access to the international trading and financial systems by malevolent Chinese and Russian space-related, state-owned enterprises (several of which are publically-traded in Western capital markets). From the perspective of international law it is essential to have a clear definition of "space hybrid operations" in order to delimit the possible reactive measures. If the space hybrid operation amounts to an armed attack in light of Article 51 of the UN Charter, a reactive measure in the form of the right to self-defence is lawful. In other words, defensive recourse to the use of force and the right of the target to strike back is legally permissive.

It raises the question, however, of how to define an armed attack in the specific physical conditions of Outer Space? Which iteration of space hybrid interferences might constitute an armed attack? Beyond conventional military attacks, other space service disruptions might be judged, most practically, similarly to cyber-attacks, via the "effects-based doctrine". It means that we assess the qualification of the attack in light of the consequences and damages caused. If a particular space hybrid disruption causes substantial harm and damages, the quantity and quality of which is equivalent to the destruction produced by a regular conventional armed attack (e.g. deactivation of data/signals paralyzing the functioning of the critical infrastructure of the state causing significant damage or even fatalities), the qualification as "armed attack" might apply. If a space hybrid operation does not attain the level of an armed attack but is qualified as illegal, there exists the right to apply countermeasures or reprisals. Countermeasure/reprisal is an act which is in itself illegal, but has been made acceptable in retaliation for the commission of an earlier illegal act by a state actor. Examples of countermeasures are traditional economic, financial or political sanctions. It is therefore essential to determine which of the hybrid disruptions constitute an international wrongful act. We may identify applicable rules banning such activities or initiate a new set of rules. If the space hybrid operation is qualified as lawful, reactive measure can reportedly only take the form of pressure or coercion called retorsion (i.e., an unfriendly and harmful act which is a lawful retaliation against an injurious activity of another state, the objective of which is to hurt the perpetrator's interests with the aim of modifying its conduct). If the space hybrid operation is interpreted as "harmful interference" (under Art. IX of OST), it is important to note that this provision does not qualify the harmful interference as such as being illegal. Art. IX of OST only lays down the legal obligation for states to resort to consultations with respect to possible harmful interference[20]. European space architectures will reduce vulnerabilities against cyberattacks and malevolent space-related economic and financial (E&F) operations; Accelerating inclusion of space in the category of hybrid threats and building space-related considerations into broader security policies – already underway – will ensure that their integration into future EU and NATO policies is bolstered by adequate funding and human resources[21].

SPACE SECURITY IN THE US

Security in Outer Space has long been a strategic interest of the U.S., compelled by the military stakes of the Cold War related to ballistic missiles

[20] *Europe preparedness to respond to space hybrid operations*, June 2018, PSSI (Prague Security Studies Institute) Report, p. 1 and following.

[21] J. Robinson, *Presentation 2018 International Astronautical Congress Session D5.4. Cybersecurity threats to space missions and countermeasures to address them Bremen*, October 5, 2018, Europe's Management of Space Hybrid Threats.

development and nuclear deterrence. Today, the U.S. SSA system is the most advanced in the world and relies on a wide national infrastructure called the U.S. Space Surveillance Network (SSN), a network of 30 surveillance sensors, including radars and optical telescopes, operated by military and civilian entities. It is the Joint Force Space Component Command (JFSCC since December 2017 – formerly the Joint Functional Component Command for Space), a component of the U.S. Strategic Command (USSTRATCOM), which, through the Joint Space Operations Center (JSpOC – recently renamed the 18th Space Control Squadron (SPCS), operates the SSN to gather, catalogue and analyze SSA data. The Centre is one of the ten joint command centers of the U.S. Department of Defense (Unified Combatant Commands of the United States Department of Defense, DoD) and is funded by the U.S. military programme. In this regard, the SSN system was originally conceived to detect objects of military significance, even though it quickly moved towards monitoring a diversity of other space objects. With ground-based radars and optical sensors located in 25 sites worldwide, SSN surveillance allows the U.S. to have unmatched mapping of orbiting objects and predict their trajectory, making interventions in advance possible, in case collisions can be predicted, or to foresee the re-entry of a body, as well as to monitor launches led by other states.

Security in Outer Space has long been a strategic interest of the U.S., compelled by the military stakes of the Cold War related to ballistic missiles development and nuclear deterrence. Today, the U.S. SSA system is the most advanced in the world and relies on a wide national infrastructure called the U.S. Space Surveillance Network (SSN), a network of 30 surveillance sensors,43 including radars and optical telescopes, operated by military and civilian entities[22].

Partial access to American SSA data is granted to selected partners through a worldwide co-operation scheme. The American approach to cooperation was updated, formalized and expanded in 2004 by the Commercial and Foreign Entities (CFE) Pilot Program and gave way, in 2009, to a full-fledged SSA Sharing Program under the responsibility of the USSTRATCOM. Today, the U.S. has more than 70 unclassified SSA Sharing Agreements with commercial and institutional organizations. These SSA Sharing Agreements aim to support transparency on operations in outer space, promote cooperation for security and safety, enhance the availability of infor-

[22] Remarks of R.H. Buenneke, *Senior Advisor, National Security*, pp. 1–5.

mation among the partners, and improve the quality of U.S. SSA information. In practice, SSA sharing agreements provide selected organizations, which are not affiliated to the Federal government, including foreign institutions and private operators, with free access to authorized data stemming from SSN sensors[23].

SPACE SECURITY IN EUROPE

The European Space Situational Awareness System (SSA) consists of three separate segments: Space Surveillance and Tracking, especially in the context of Space Debris (Space Weather) and Near Earth Orbit (NEO) observation. The European SSA system has dual-use civilian and military applications. Additional components to the SSA system may be added in the near future. They are built on the basis of military requirements and compiled by the European Defence Agency (EDA). The conference also devoted a lot of space to the development of the STM (Space Traffic Management)[24] system, which does not yet exist in Europe, unlike the USA. The goals for Space Situational Awareness are the following: society heavily dependent on critical space and ground assets, critical assets need to be protected against adverse effects from space, SSA Programme Declaration calls for independent European access to SSA data and services. There are three main areas: Space Weather, Near Earth Objects, Space Debris clean space. The participants in ESA SSA programs are 19 participating states. The good progress in the development of a SSA system in Europe has been observed and many actors involved: Member States, ESA, and EU. Distribution of roles needs to be finalized: development vs exploitation. There is still a performance gap in surveillance radars that is why there is a need to agree on a suitable governance scheme for the exploitation of future high performance European surveillance radar. There is a development of a high performance radar can be achieved within 3 years SWE and NEO systems will reach pre-operational status by 2020[25].

---

[23] ESPI Vienna report 64.

[24] STM: "Space Traffic Management (STM) is the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and return from outer space to Earth free from physical or radio-frequency interference".

[25] N. Bobrinsky, *Presentation Forging ahead: from SSA to space safety*, in: 12th ESPI Autumn Conference, 27th of September, Vienna 2018.

Thus, Europe has started its own preparatory programme of the SSA. International negotiations on permanent exchange of information and coordination, mainly with the USA, are also foreseen. Poland should also participate in these studies, which this year is to eventually become a member of the European SSA Consortium, where they play the biggest role: France, Germany, Great Britain and Italy. Much of the data to be dealt with by the established Consortium can be found in public satellite catalogues created by the USA and other countries, which are available on the Internet and can be freely used. That is why transatlantic cooperation is so crucial. Orbital paths are constantly changing or are disturbed by a number of factors, such as inconsistent degrees of attraction, solar activity or the effects of gravity of other orbital objects. International cooperation on SSA data sharing is weakened by issues such as liability and property concerns, data formatting standards and compliance with catalogued tools, and finally security (some satellites do not provide data to the public). These issues are still being discussed in various international fora, including UN COPUOS (United Nations Committee on the Peaceful Uses of Space). The author follows these discussions on an ongoing basis and makes use of them in her scientific work. Space security has a multidimensional concept. It can be understood as Security in Outer Space, Outer Space for Security or Security for Space. The first means the protection of the space infrastructure against natural and man-made threats or risks, ensuring the safety and sustainability of space activities. The second means the use of space systems for security and defence purposes. Security for Space means the protection of human life and the Earth environment against natural threats and risks coming from space.

There are also several meanings of such definitions as: Space Situational Awareness (SSA) which can be understood as current and predictive knowledge and understanding of the outer space environment including space weather and location of natural and manmade objects in orbit around the Earth; SEPP (Space Environment Protection and Preservation, which is preventive and curative mitigation of negative effects of human activity in outer space on the safety and sustainability of the outer space environment and Space Infrastructure Security (SIS) as assurance of the infrastructure ability to deliver a service that can justifiably be trusted despite a hazardous environment.

There are some challenges to space infrastructure security, such as unintentional hazards (space debris, accidental interferences), Intentional threats (ASAT, malicious interferences, and cyberattacks), Space weather hazards (geomagnetic storms, solar storms).

There are rising challenges to space infrastructure security. Space is an increasingly congested and contested resource. Space is multiple and diverse, there are different mitigation and protection measures. There are many actors playing in the Space, so interdependence between them has been noticed. There are various trends in Space, such as increasing space activity, new concepts, connected space, strategic target, "space control" capabilities, etc. The most important is growing dependence on space for society and economy at large[26].

Growing security threats to civilian space programmes (access to space, cybersecurity in space, safe operations in space). Space is a critical infrastructure: satellites (jamming, spoofing, blinding), ground stations (hacking). Threats (military, non-military, natural) are understood and accepted and now are more properly and precisely assessed. Readiness to face and respond to threats is growing in governments and private sector. It seems that there is a possibility to invest in handling threats are developing and to find political solutions in managing threats[27].

FINAL REMARKS

To sum up, all EU Member being active in Space will need to take the urgent steps to implement the SSA into national system of law. The US example and its experience can be a good one to follow. The system will guarantee some privileges such as sharing data and cooperation among states which is crucial in undertaking any kind of space activities in dual use meaning, mostly in preserving security. Thus the urgent steps should be done to make SSA system in force as soon as necessary.

REFERENCES

"The status and future evolution of Transparency and Confidence Building Measures." 2010. In: *The prospects for Transparency and Confidence-Building Measures in Space*, edited by Jana Robinson, Michael P. Schaefer, and Karl-U. Schrögl [et al.]. Vienna: ESPI Report 27.

Al–Ekabi, Cenan, and Stefano Feretti. 2018. *Yearbook on Space Policy 2016 – Space for sustainable development*. Vienna: ESPI.

[26] S. Moranta, *Security in Outer Space: Perspectives on Transatlantic Relations*, in: *12th ESPI Autumn Conference*.

[27]K. Uwe Schrögl, *Security in Outer Space: Rising Stakes for Civilian Space Programmes*, in: *12th ESPI Autumn Conference*.

Bobrinsky, Nicolas. 2018. "Presentation Forging ahead: from SSA to space safety." In *12th ESPI Autumn Conference, 27th of September*. Vienna: ESPI.

Buenneke, Ronald H. 2018. *Senior Advisor, National Security Space Policy Office of Emerging Security Challenges Bureau of Arms Control, Verification and Compliance U.S. Department of State Panel on "Balancing national security and economic security in a contested and congested space domain" "Greater Security Through International Space Collaboration" Seminar George Washington University Space Policy Institute The Aerospace Corporation's Center for Space Policy & Strategy*.

Cour–Palais, Bourton G., and Donald J. Kessler. 1978. "Collision frequency of artificial satellites: The creation of a debris belt." *Journal of Geophysical Research* 83:2637–2646.

Faiyetole, Ayodele A. 2018. "Potentialities of Space-based Systems for Monitoring Climate, Policies and Mitigation at Climate Policies and Mitigations of Climate Process Drivers." *The International Journal of Space Politics and Policy* 14(8):28–48.

Harrison, Ross G. 2013. "Unpacking the Three C's: congested, competitive and contested Space." *The International Journal of Space Politics and Policy* 11(3):121–131.

Klein, John J. 2012. "The influence of Technology on Space Strategy." *The International Journal of Space Politics and Policy* 10(1):8–26.

Moranta, Sebastien. 2018. "Security in Outer Space: Perspectives on Transatlantic Relations." In *12th ESPI Autumn Conference, 27th of September*. Vienna: ESPI.

Othman, Mazlan. 2017. "National Space Policy and Administration." In *Handbook for New Actors in Space*, edited by Christopher. D. Johnson, 54–87. Secure World Foundation.

Paracha, Sobia. 2013. "Military dimensions of the Indian Space Programs." *The International Journal of Space Politics and Policy* 11(3):156–186.

Polkowska, Małgorzata. 2018. Prawo bezpieczeństwa w Kosmosie. Warszawa: Instytut Wydawniczy EuroPrawo.

Radtke, Jonas, Christopher Kebschull, and Enrico Stoll. 2017. "Interactions of the space debris environment with mega constellations – Using the example of the OneWeb constellation." *Acta Astronautica* 131:55–58.

Robinson, Jana. 2018. *Presentation 2018 International Astronautical Congress Session D5.4. Cyber-security threats to space missions and countermeasures to address them Bremen*. Europe's Management of Space Hybrid Threats.

Schrögl Uwe, Karl. 2018. "Security in Outer Space: Rising Stakes for Civilian Space Programmes." In *12th ESPI Autumn Conference, 27th of September*. Vienna: ESPI.

Wyler, Greg. 2017. "Responsible Operations in Space." In *Handbook for New Actors in Space*, edited by Christopher. D. Johnson, 88–132. Secure World Foundation.

PRAWO BEZPIECZEŃSTWA: SYSTEM ŚWIADOMOŚCI SYTUACYJNEJ W KOSMOSIE (SSA) W STOSUNKACH TRANSATLANTYCKICH. EUROPA A USA

Streszczenie. Niniejszy artykuł dotyczy bardzo delikatnej kwestii, takiej jak bezpieczeństwo kosmiczne i jego pilnej potrzeby wdrożenia do prawa krajowego. Istnieje szereg wyzwań dla bezpieczeństwa infrastruktury kosmicznej, takich jak niezamierzone zagrożenia (śmieci kosmiczne), zagrożenia celowe (broń kosmiczna, umyślne zakłócenia, ataki cybernetyczne) lub zagrożenia związane z pogodą w przestrzeni kosmicznej (burze geomagnetyczne, burze słoneczne, itp.). Z drugiej strony, rośnie zależność od przestrzeni kosmicznej niektórych państw, w tym państw europejskich. Istnieje zatem pilna potrzeba przyspieszenia prac nad bezpieczeństwem i współpracą międzynarodową, np. między Europą a USA – „liderem kosmicznym". Współpraca transatlantycka w dziedzinie prawa bezpieczeństwa kosmicznego ma kluczowe znaczenie. Stany Zjednoczone posiadają niezbędną wiedzę w swojej długiej historii w zakresie tworzenia strategii kosmicznej, polityki i prawa bezpieczeństwa i mogą być dobrym przykładem dla Europy w budowaniu struktur bezpieczeństwa w Kosmosie.

Słowa kluczowe: bezpieczeństwo kosmiczne, system świadomości sytuacyjnej w Kosmosie, prawo kosmiczne, strategia kosmiczna