ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2018. Випуск 44 С. 119–134
Visnyk of the Lviv University. Series International Relations. 2018. Issue 44. P. 119–134

УДК 327:
DOI dx.doi.org/10.30970/vir.2018.44.0.9467

NON-STATE ACTORS AND SPACE SECURITY

Marek Czajkowski

Uniwersytet Jagielloński,
ul. Gołębia 24, Kraków, Poland, 31-007, tel. : +48- 12 663 10 46,
e-mail: marek.czajkowski@uj.edu.pl

Human presence in outer space is closely related to national and international security – space applications have become tools of choice for many kinds of tasks performed by militaries since the early sixties of XXth century. Military use of space is therefore something obvious and common, but non-military activities affect international and national security as well. To address all the problems associated with that a special term has been coined, «space security». It refers, generally speaking, to all the security issues related to outer space.

Current phase of advance of the space exploration and exploitation may be characterized, among others, by ongoing proliferation of related technologies. This refers to spreading of capabilities among growing circle of nations, but also to non-state actors of international relations. Thus, the latter have already attained capabilities to adversely affect orbital systems and they will they are grow rapidly in coming decades. Therefore space security, narrowly understood as safety of space-borne man-made objects and their capability to operate uninterrupted is increasingly jeopardized. This paper refers to one of the specific issues related to space security, which is a role of non-state actors within this area. Therefore, we intend to study the impact that such actors have upon space security related issues – it is going to be the main goal of this article. To achieve this the paper depicts an analytical framework regarding understanding of terms «space security» and «non-state actor», describes the activities of non-state actors that may result in increasing threats to space security and assesses the relation between space security and non-state actors, drawing some general observations related to international security as a whole.

Key words: International Security; International Relations; Space Security; Non-state Actors; Outer Space; Spacepower.

For over six decades the Mankind has been perfecting its abilities to harness outer space for various purposes which had been envisaged even before the first orbital craft was launched on October 4th, 1957 [17]. At a dawn of the Space Age this expensive and complex venture into the unknown was available only to the richest and the most determined governments. Understandably, they initially turned their attention to the applications that would have been useful as tools fostering states' main functions. Particularly promising were the ones which concerned the realm of national security, especially because the cold war was on the rise and threats it had spawned became a centerpiece of security policies of the main adversaries. In the next decades however, space-borne systems became increasingly employed for non-military functions via state-owned civilian agencies and nongovernmental commercial organizations. Gradually, their use became indispensable in almost all the fields of human activity. Especially the last decade or so saw rapid growth of space systems' relevance, as

«[m]illions of individuals rely on space applications on a daily basis for functions as diverse as weather forecasting, navigation, and search-and-rescue operations»[20, p. 12]. As of 2016, space related industry was worth 329 bln USD worldwide, and it was expected to grow fast in years to come [18].

Today, human presence in outer space is of course still closely related to national and international security – space applications have become tools of choice for many kinds of tasks performed by the militaries since the early sixties of XXth century. Military use of space is therefore something obvious and common, but non-military activities affect international and national security as well. To address all the problems associated with that a special term has been coined, «space security». It refers, generally speaking, to all the security issues related to outer space, although we must note that it is still quite vague and imprecise expression.

This paper refers to one of the specific issues related to space security, which is a role of non-state actors within this area. It seems quite important, as this kind of players of the international stage have become increasingly significant in the world affairs. We intend to study the impact that such actors have upon space security related issues – it is going to be the main goal of this article. To achieve it we will first of all depict an analytical framework regarding understanding of terms «space security» and «non-state actor». Then we will describe the activities of non-state actors that may result in increasing threats to space security – we will stress a prognostic dimension of the issue. And finally we will assess the relation between space security and non-state actors, drawing some general observations related to international security as a whole.

1. Analytical Framework

As it has already been mentioned, the term «space security», central for this paper, is not clearly defined. There are many competing understandings of it, some scholars do not even use it at all. For example, spacesecurityindex.org, a respected organization monitoring space related security issues provides a general definition of space security, stating that it means «[t]he secure and sustainable access to, and use of, space and freedom from space-based threats» [20, p. 1]. This definition stresses a transnational approach in the spirit of commonality, contrary to the other, narrow view of the issue as a matter of an individual state's interest. The latter is adopted mainly by theorists of the realist denomination, that even do not use the expression «space security», preferring «spacepower» instead – the term that applies to nation-state and its capacities [6].

We are certainly not going to immerse in a theoretical discussion with intent to solve the differences and produce overarching definition. This part of our paper is supposed only to depict our view on the matter and to present the definitions of the most important terms that we endorse.

When the phrase «space security» is used it usually means first of all the issues related to human activities in outer space – this is the first and obvious intuition. In practice it does mean use of various devices placed in the space domain, but none of them is detached from Earth's reality, none works for itself. Satellites serve human activities that are inseparably tied to the man's natural environment which is the Earth.

Although a label «space security» suggest something «extraterrestrial» it is no such thing, for in essence the term applies to our planet. Thus, while using it we refer to the problem of human activities carried out in outer space, but which influence broadly understood «terrestrial» security.

More specifically, space security may be explored from various points of view, particularly from the two main perspectives: one is international security as a whole, and the second refers to national security of individual states. And so, on one hand we would refer to this portion of the international environment which is more or less tied to outer space and to generally outlined threats to use of space. It is therefore a broad, holistic perspective, strongly accentuating synergy of complex relations between international actors. On the other hand, we would refer to narrowly understood national security of an individual state performing its protective function – space activities will therefore be treated as just another instrument that state wields. Of course, this tool is not only useful within military and political domains but works also in an economic one, fostering growth of state's power. And here the traditional realist approach applies intuitively and the term «spacepower», understood as a capability of state to benefit from space activities, emerges as central. Both of these two perspectives may also be applied within broader context of global or regional international relations or bi- and multilateral interactions.

A structural analysis may also be applied to space security to describe and evaluate certain areas of countries' and non-state actors' activities, as they act along strategies designed for own security, simultaneously impacting security of others, either directly or through influence on the security environment. Here three distinct structural approaches may be proposed: «security in space», «security through space», and «security of space related ground-based infrastructure».

«Security in space» refers to safety of space-borne objects – note that currently almost all of them are located in Earth's orbit, but it will change in future. They are supposed to function in hostile environment of space, exposed to multitude of threats, both natural and man-made. Relatively fragile satellites may be damaged or destroyed by radiation, impact of celestial bodies, atmospheric drag, and intentional or accidental influence of individuals, organizations or state-owned entities .

«Security through space» is of course closely related to the abovementioned perspective, because one can think of using space for any purpose only when safety and proper functioning of satellite systems is secured. Consequently, this approach means first of all use of space systems as an instrument of national security. It may also be more generally understood as an element of «spacepower», which is a multifaceted ability of state to benefit from space activities – not necessarily through actual doings of its bodies or agencies but through general economic, technological or social development as well. In a broader, international context, unhindered use of satellites is also functional for overall economic growth and for widely understood international security. The other important aspect with respect to that is human or social security, since orbital systems are increasingly critical as communication devices, particularly because they support Internet with its social function. This will soon intersect even more profoundly than it currently does with a sphere of countries'

internal security. Establishment of easily accessible satellite worldwide Internet services will surely add to the difficulties of controlling societies by authoritarian regimes that struggle to rule their own internal information spaces [7].

And finally, «security of space related ground-based infrastructure» does not refer directly to orbital crafts although it is in fact critically important for their utility. It is because every space system consists of three basic elements: spacecraft, ground-based infrastructure (not to be confused with devices used to receive services provided *via* satellites) and the link between them for control and data transmission. This infrastructure may be understood narrowly as an equipment which is devoted to controlling satellites – this is the most common approach. But broader definition may be applied as well, so we can add space related production, R&D and education facilities to this category.

It is worth to emphasize at this point that the abovementioned approaches should be treated as neither complementary nor disjunctive. They are three specific levels or planes of analysis that may be used separately according to the specifics of analyzed object and/or needs of research goal. But they may also be combined to create synthetic picture from wider perspective – a sort of two- or three-dimensional approach. Consequently, this paper refers only to security in space, because we are not going to analyze various functions and tasks that satellites perform. We are rather interested in their operation itself and in the threats to it – with an eye on some final conclusions related to international security as such. However, for the sake of comprehensiveness we will frequently mention other approaches as well.

The "non-state actors" is a vast category, relatively difficult to define synthetically within the realm of international relations. Usually we use this term referring to organized groups, politically independent from state which have their own political goals. Within a state it is relatively easy to single them out, pointing to their legal position *vis-a-vis* a government's apparatus. On the international arena it is far more complicated, because we refer, as a rule, to actors that act within the international space defined by interactions among states but they are no states. The main difficulty is to precisely characterize their interface with states, especially what is "internationality" or "externality" of non-state actors from states' perspective. Note, that in practical terms they function, at least partially, in accordance with laws created by states (e.g. multi-national corporations), or outside the law or even against it but still with the law as a crucial point of reference (e.g. criminal organizations or terror groupings).

Without further discussion on definitions we will simply enumerate entities that we label the non-state actors of international relations. Apart from classic intergovernmental organizations, which are obviously situated within this category, there are following types of non-state actors: corporations, worldwide independent media outlets, social networks, non-governmental international organizations, transnational crime organizations, terrorist groupings and rebel movements[1]. We have to stress that all the categories listed above consist of subjects that can but do not have

[1] Sometimes a category «individuals» is added, but it is difficult, even if possible, to build convincing case for such an approach.

to be non-state actors in the sense of international relations. Everything depends on their identity, goals and aims, and actions they undertake – but to determine at which moment a given entity becomes international actor is very difficult. Therefore there should be no automatism while recognizing non-state actors, every instance should be deliberated separately.

From a point of view of space security non-state actors may be considered relevant within each of the three abovementioned approaches. They can affect security in space by disrupting functions or even destroying orbital crafts either by direct or indirect influence. Security through space may be compromised when non-state actors' actions result in limitation or even disconnection of satellites' functions used for purposes of national security. And security of ground-based infrastructure may be endangered through disruption of its facilities' functionalities through physical or virtual damage or destruction.

In every of the abovementioned approaches we can also select two important dimensions. Firstly, there is a point of view of those who are interested in space security for the sake of safety of their own activities which involve use of satellite systems (e.g. banks and corporations, especially the ones providing broadcasting services). Secondly, there are actors that intent to endanger safety of space systems, adversely affecting space security (e.g. criminal organizations, terror groupings or separatist movements). This also refers to legally existing entities that perform illegal or semi-legal operations (e.g. private security firms or shadowy organizations performing murky services in cyberspace, sometimes informally linked to nation-states). From this point on we will refer to the latter group of non-state actors, recognized as a threat to security in space.

2. Non-State Actors as a Threat to Security in Space

Generally speaking, all of the three components of space systems (orbiters, data links and ground infrastructure) may be endangered by various actions directed against them. Satellites can be damaged, even destroyed, or their functions may be impaired. Ground-based infrastructure may be damaged or destroyed as well with adverse effect for orbiters. The same refers to the link connecting satellite with its command structure which may be disturbed or even severed; it can also be eavesdropped or spoofed, what does not endanger the system directly but effects with diminishing or negating its usefulness.

From a point of view of security in space, what in essence means safety of spacecrafts in orbit, all of the abovementioned threats should be regarded as important factors, but

«[u]ntil fairly recently, an adversary attempting to disable a satellite system needed either to destroy the system's ground station or to target the satellite itself, usually with an anti-satellite (ASAT) missile or a powerful Earth-based jammer. Generally, only well-financed and sophisticated state actors were able to acquire and deploy these weapons. As a result, it was possible to attribute responsibility for attacks with relative ease and certainty» [10].

Anti-satellite capabilities of superpowers were therefore just a part of global military balance within the bipolar system and they were treated as such during a

course of the cold war. But this relatively simple situation has changed dramatically in the last decades as negation technologies matured and became more accessible. Today, not only many more countries may attempt to adversely affect space systems, but even some non-state actors are able to do it. This developments add countless variables to the security equation on regional and global scale, so let us see what are the capabilities that are available to non-state actors that can endanger security in space.

There are three methods of compromising space systems, and all of them are available to non-state actors, at least to an extent. Firstly, a computer based attack through cyberspace may be attempted, what in fact means influencing a software of a space system in order to trigger a certain adverse effect, including destruction of the spacecraft. Secondly, an interference with use of electromagnetic beam directed against one or more of elements of space system may be created; an orbital component is especially exposed to this kind of influence, so spacecrafts may be destroyed or their functions disturbed. And thirdly, kinetic attack directed to damage or destroy spacecraft may be performed – here the most vulnerable is ground-based component, but orbital crafts may also be hit. Additionally, it is possible to intercept or spoof data via virtual operations in cyberspace or via tampering to communication link with ground-based or space-based antennae.

The influence on space systems through cyberspace is achievable because they are connected to the Internet in multiple points *via* communication protocols, and that «[…] has made them vulnerable to a variety of new forms of attack. Using the Internet to perform certain satellite communications functions allows would-be bad actors a variety of low-cost opportunities to access both ground stations and satellites. Almost any tech-savvy hacker is now a potential threat, and a successful hacker can do more than simply damage or destroy the satellite itself. The hacker can also deny, degrade, or counterfeit the satellite's transmissions; access and leak imagery and other data collected by satellite sensors; or compromise other terrestrial or space-based networks used by the satellite. Without pervasive situational awareness and advanced technical attribution tools, perhaps complemented by other non-technical forms of information gathering, the attacker's identity, affiliation, and location may never be known» [10].

There is a long lists of actual attacks of that sort which exploited a number of vulnerabilities, especially of commercial satellite systems – many of them may be attributed to non-state actors. Most of such events resulted in negative impact, many had important security related consequences [16, p. 33–41]. Chatham House experts provide following typology of cyber threats and methods of anti-satellite virtual attacks:

«Cyberthreats against space-based systems may be classified as follows:

– States setting out to create military advantages in space, or seeking to steal strategic quantities of intellectual property and having sufficient computing power to crack encryption codes, for example;

– Often well-resourced organized criminal elements seeking financial gain;

– Terrorist groups wishing to promote their causes, even up to the catastrophic level of satellite collisions with space debris including a cascade of collisions – called the Kessler Effect[2], denying the use of space for all actors;
– Individual hackers who simply want to prove and fanfare their skills;
– Any combinations of the organizations and individuals above.
And their methods would be:
– Jamming, spoofing and hacking attacks on, for example, communication networks, by using space infrastructure;
– Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby 'weaponizing' it), or 'cook' or 'grill' its solar cells through deliberate exposure to damaging levels of highly ionizing radiation;
– Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example on weather forecasting systems, which use large quantities of space-derived data)» [12, p. 9].

Electromagnetic form of influencing satellite systems may be executed in two ways. First one is an interference with communication signals by jamming it, second is blinding or damaging satellites with a laser or, potentially, a microwave beam. Jamming of satellite signal is relatively simple, as a rule it requires use of a transmitter powerful enough which works on applicable frequency, and is located at a suitable place to «cover», or «envelope» a communication signal. The most vulnerable are of course civilian systems, because military ones are expected to execute their task in the electronic warfare environment. To jam them effectively it is necessary to possess more sophisticated and less available devices – but this does not mean that they are out of reach for non-state actors. Laser dazzling or blinding satellites is similarly accessible. To attack satellite this way it is necessary to employ tracking devices which are available on the market in a form of amateur telescopes equipped with computer controlled mounts connected to open source databases and supported by easily accessible software [2]. Such a telescope can be supplemented or replaced with industrial low-power laser.
«Low-powered lasers have been used to «dazzle» or degrade unhardened sensors on satellites in LEO. In 1997 a 30-watt laser used for alignment and tracking of a target satellite for the megawatt U.S. Mid-Infrared Advanced Chemical Laser (MIRACL) was directed at a satellite in a 420-km orbit, damaging the satellite's sensors. This suggests that even a commercially available low-watt laser functioning from the ground could be used to «dazzle» or temporarily disrupt a satellite» [19, p. 74].

And finally, a kinetic effect on satellites means damaging or destroying them through an impact of a solid body, be it a splinter from the explosive fragmentation warhead or a hit by the dedicated interceptor. We may safely assess that both classic ASAT methods, which are described below are more or less available to non-state actors.

[2] Theoretical concept of a cascade effect caused by destruction of satellites which produce debris that in turn destroy other satellites causing even more debris and so on – much like chain reaction of fissile elements.

Firstly, co-orbital, «[s]atellite-to-satellite attacks enabled by the proliferation of inexpensive nanosatellites that are easy to launch and hard to detect, particularly in high orbits […]» [10] could be employed. Such satellites are commercially available – properly instrumented and generously filled with fuel to maneuver may pose grave danger to other satellites. Obtaining such a «killer-sat» would not be an easy task, but given that there are so many organizations and companies that produce items of that kind it is conceivable that some of the most sophisticated, well connected and rich non-state actors can manage to get it. Placing such weapon into orbit is also complicated, because of national and international regulations pertaining to registration of satellites, but the control system is not impenetrable [8]. Thus, it is possible that small satellites which could be used against the other orbital crafts actually are in, or soon may come into possession of malevolent non-state actors. The variant of this method is taking a control over someone else's satellite already in orbit in order to use it as a ram. The greatest limitation of this method is inherently insufficient maneuverability of satellites, especially small ones that naturally have limited capacity to store fuel. This means that an individual «killer-sat» would have to be inserted into orbit close to the intended target – and this can be of great difficulty in technical and organization sense. It is because a non-state actor should either have full control over whole launch and orbital insertion procedure – it means in practice the possession of own launch capabilities – or be able to deflect obvious suspicions of launch operators and state registration agencies which control space traffic. Furthermore, setting up a ground control network would also be difficult, but still not impossible, given availability of related software and hardware.

Secondly, a non-state actor may use some variant of a direct-ascent method to perform an anti-satellite attack. This technique involves launch of an interceptor missile from the ground with the mission to climb to a certain point of orbit where a satellite would be in a certain moment in time. If both trajectories are properly calculated and missile controls perform well, flight paths of a kill-missile and a satellite cross and the spacecraft is destroyed by impact of missile itself or some kind of splinter from it. The main obstacle is of course a guidance system which requires extreme sophistication, especially with regard to hit-to-kill warheads. To relax this restraint somehow a pellet-ASAT may be employed – the technology that was considered already during the cold war. This method involves a missile with the warhead which releases a cloud of small pellets (several centimeters of diameter would be enough) that expands on its way up – at the moment of crossing the satellite's path it may be even hundreds meters in diameter, greatly increasing the chance to hit a target satellite. Of course there is a number of technical problems before such a venture, but given the availability of satellite databases, optical computer assisted tracking systems, and laser ranging devices it is conceivable that non-state actors would come into possession of such systems. Of course, this method requires a relatively powerful missile, but this technology proliferates very fast, with countries like North Korea, Iran or Pakistan as likely sources. Note, that even the first German V-2s were able to reach orbital altitudes, so it is not necessary for non-state actor to look for big space-launch rocket. Medium range ballistic missile should be

powerful enough to send sufficient number of pellets into a low earth orbit. The greatest challenge with respect to that is not power of the missile but rather its guidance and control systems that should be good enough to be able to execute flight along precisely calculated path in precisely calculated time. It is difficult to determine if such a technology is doable for non-state actors, but the components necessary are accessible, and their integration seems possible – especially with a proper dose of help from nation-states or their agencies, be it intentional or non-intentional (by theft or leak for example).

In addition to anti-satellite potential or actual capabilities of non-state actors, they can also perform attacks against ground-based space system's infrastructure, as «[s]atellite ground stations […] are vulnerable to a range of widely available conventional […] weapons. While military satellite ground stations […] are generally well protected, civil and commercial assets tend to have fewer protective features» [19, p. 69].

As we can see, there are many ways by which non-state actors who possess specialized but not really arcane knowledge and commercially available data processing equipment might disrupt satellite operations or even cause the destruction of spacecrafts. Actions that involve some pieces of hardware, obtained legally or by theft, are also within reach of some more advanced, wealthy and well organized non-state actors, especially if they have good connection to nation-states that would be willing to help or would unintentionally leak technology or pieces of equipment.

In the worst case scenarios non-state actors, by the way of «[t]he application of some destructive space negation capabilities, such as kinetic-intercept vehicles, would also generate space debris that could potentially inflict widespread damage on other space systems and undermine the sustainability of outer space» [19, p. 18]. It refers to the already mentioned Kessler effect which could cause pollution and degradation of at least some portions of near-Earth space.

3. Consequences

Growing significance of non-state actors within the realm of space security stems out of two intersecting factors. First of all we must notice overall increase of relevance of players of this kind for the international stage. It is caused by demand for international subjectivity that is on the rise among non-state groups and organizations, and which originates from growing and evolving human aspirations. Groups of people seek opportunities to realize their political, economic and social interests and aspirations and they circumvent state in the process. Even if they act in most cases inside a state, they autonomously specify their interests and independently seek the ways to realize them. Today those ways lead, among the others, through transnational activities that broaden groups' and organizations' perspective and perception of their goals and aims. Therefore they enter into interactions with state, so to say, «from outside», that means as actors which are not fully controlled within a framework of state's internal order. Thus, non-state actors are able to autonomously formulate their goals and aims and to realize them regardless the will of state, in the international arena as well.

The second important factor is the evolution of space applications and their relations with «terrestrial» technology. Especially important is spreading of the Internet and connecting space systems into it, in the form of Internet of things as well. The technologies which increase accessibility of outer space are functional to dissemination of use of space systems, this in turn increase ease with which they can be utilized by non-state actors. The most profound developments with regard to that are: advent of small satellites which have relatively broad capabilities, spreading of orbital systems tracking and control software and hardware, and lowering of the cost of launching a proverbial 1 kilo into orbit. All those developments, especially diminishing of a launch cost, are supposed to continue in future. One of the most important consequences is that state agencies, big corporations or international scientific bodies have lost their monopoly to use satellite systems. Today small satellites are launched for smaller companies, universities, the road is also opened for individuals to procure and possess orbital crafts [5]. The amount of such spacecrafts grows every year, currently there are over 500 of them in orbit[3], and their number is supposed to multiply by the factor of 10+ in less than a decade [11]. These developments open vast opportunities that non-state actors may use for various kinds of wrongdoings. The single biggest obstacle that lie before malevolent non-state actors in obtaining independent space capabilities is the already mentioned state controlled registration procedure and state's control over space launches. Although firmly established in the national and international space law[4], this system is not impenetrable, as it has also been mentioned above. Criminal organizations, terror or rebel groupings are therefore by no means capable of creating own space systems which could endanger space security. It is even conceivable that such systems already exist.

Thus, non-state actors do have a great number of tools which they can use to adversely influence space security, and it is in fact just one of displays of their increasing role and capacity. Not only in space, but everywhere else they crush state monopoly to use state-of-the-art technologies – it means that the solutions available for them are in many cases as good or even better than the ones that are in governments' inventories. Thanks to that, the superiority that state possesses over non-state actors is thinner and thinner and in multiple cases disappears, sometimes even morphs into the opposite. What is more, non-state actors are usually more flexible, act faster, and adapt quicker thanks to organization simpler than that of state. They are also able to ignore some of the limitations that hinder state's actions – especially complex bounds of the legal system. This adds up with technological prowess of non-

[3] As of January 1, 2018, 560 satellites qualified as nanosats were in orbit. Note that the classification we quote here is somehow complicated, so let us assume that the term «nanosat» refers to satellite usually smaller 35 kilos [14].

[4] The basic documents with regard to registration of space objects are: Outer Space Treaty of 1967 (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies – OST) and Registration Convention of 1967 (Convention on Registration of Objects Launched into Outer Space – REG).

state actors, furthering their capabilities and influence in international relations, enabling them to employ various asymmetric tactics – sometimes even giving them an advantage over state.

It can therefore be concluded that non-state actors compromise space security with increasing frequency and with rising number of methods. The most profoundly it happens through activities in cyberspace directed against orbital systems, but also through physical influence both from the ground and through utilization of own space systems. This problem is on the rise and may have multifaceted impact on international security. The most significant manifestations of this impact are as follows:

– non-state actors' ability to negate space capabilities of state empowers them even more and make them be even more dangerous and momentous for space security and in turn for international security as a whole; consequently more and more non-state actors are and will be tempted to develop own space capabilities to emulate the capabilities of states used for security related purposes;

– the capability to physically destruct satellites, either by hacking, by influence from the ground, or *via* co-orbital or direct-ascent ASAT may lead to rising pollution of already congested orbits – in the worst case scenario it may lead to significant difficulties or even to preventing of use of certain territories in near-Earth space; this in turn will compromise international security in many forms because of disturbances or even cessation of use of assets important to maintaining international security;

– distractions of space systems' functioning caused by non-state actors' activities, even if directed mostly against states may adversely affect commercial space applications [21] and their social functions; this would impact international security in its economic and human dimensions;

– it may come and probably it actually comes to a sort of «outosurcing» of hostile actions in space, that involve non-state actors which temporarily or permanently act for nation-states in a form somehow close to classic mercenary service; such actions would be convenient for some countries because of the same reasons that make private contractors be a tool of choice for states on countless occasions; it may even be institutionalized in forms of clandestine symbiosis of nation-states and cyberspace dwelling non-state actors for the activities in outer space.

As a general consequence, governmental bodies and commercial entities alike, which are constantly being attacked by non-state actors that use increasing range of methods, are compelled to devise more and more sophisticated counteractions in the space domain. It not only brings significant price-tag, but is also very difficult – the adversary employs flexible tactics and strategies and uses versatile methods, many of them are commonly available off-the shelf.

On the other hand there are of course multiple means to increase resilience of space systems.

«The satellite itself may be hardened against radiation, micrometeoroids, and orbital debris. Ground stations can also be physically reinforced to protect against natural disasters and kinetic attacks, equipped with high-power radio uplinks that are difficult to jam or overpower, and use other physical and cyber security controls.

Communications signals may be encrypted, employ unique satellite-specific digital interfaces, and be spread across a wide band of the radio spectrum. To minimize disruption in the event that a single satellite or ground station is disabled, satellite networks may use multiple satellites and ground stations to provide redundancy» [10].

It is especially necessary to secure military systems, and so new ones are designed as more robust, older are being safeguarded [22]. Although by their nature they are less prone to interference, they are not immune to non-state actors' attacks. The effort is also being made to improve a capability to quickly reestablish functioning of space systems after they were attacked. This refers to all of the components of space systems and methods range from creating redundant orbital capabilities, storing additional units ready to launch, through designing versatile launch systems able to respond quickly and place new satellites in orbit, to overcapacity of ground systems and contingency planning for fast rebuilding of infrastructure. Yet, all of this may not be enough, and therefore it is also necessary to prepare to live with impaired space systems or even without them. That is why «[g]overnments are slowly investing in shielding electronics, building «reversionary modes» (or backup systems), and training personnel to operate for prolonged periods without the basic communication, navigation and other space-dependent services that underpin so much of digital living. Beyond government, some organizations are developing space security and response plans to mitigate the effects of a loss of space services. Militaries, shipping companies and logistics firms are investing in inertial guidance systems as a substitute for GPS. Moreover, Airbus and Facebook are two companies that have suggested using solar-powered drones or high-altitude aerostats to provide internet connectivity and other «pseudo-satellite» services as an alternative to reliance on space» [4].

Perhaps the most important dimension of counteracting non-state actors' space negation capabilities is international co-operation. It looks somehow obvious, as space-faring nations apparently have common interest in space safety. They all have their important systems in space, therefore they all could be compromised by increasingly available space capabilities of non-state actors. The most universal threat is the Kessler effect which would render many instruments crucial for countries' strategies and policies permanently unusable. This refers also to non-space-faring actors, because they are depended on space systems in many ways as well.

Unfortunately, nation-states' willingness to curb non-state actors' space negation capabilities cannot be taken for granted. For two reasons. Firstly, for many countries, cyberoutsourcing which might be employed in outer space as well, is an important tool of influence, both externally and internally; sometimes it is even a weapon of choice within asymmetric or hybrid strategies. Secondly, international technology flow control regimes are difficult to construct and to implement; they are also often considered by less developed countries an instrument devised by «the evil West» to hamper their development and keep them backward.

The other, somehow separate problem of international cooperation beyond Earth is that the space law is especially weak within the realm of international security and there is general unwillingness among states to augment it substantially. Even in the United States, the country that should be the most interested in space safety because it

is so deeply dependent on space systems, an aversion to the new regulations and universal international rule-based co-operation is surprisingly widespread. It is mainly because it is considered by many in the U.S. that any agreement on furthering space law is a concession to the foes and a restriction imposed on America, which is currently leading in space in pursuit for its vital interests.

However, international co-operation has its important positive dimensions, and it would surely be

«[…] crucial in any response to space-based cyberthreats, and is at the heart of current debates, for the following reasons:

– Large numbers of satellites orbit the Earth, traversing all territories, and their uplinks and downlinks are transmitted via ground stations from all around the world;

– These satellites are used worldwide, whether for communications, Earth observation or precise navigation and timing capabilities;

– Satellites are built with components from an internationalized supply chain» [12].

The remarks above certainly refer not only to the cyberspace, but also to the other threats that are posed by non-state actors. And that is why, despite many obstacles, international co-operation with regard to space security is visible in many practical issues – and that prompts some optimism [13, p. 90–96]. All in all it is a necessity that stems out from the most general physical properties of outer space and related technologies, and from numerous practical and economical reasons.

Conclusion

Probably the most profound feature of a current phase of the Space Age is that Earth's orbit, especially its lower layers is opening to a host of new users. Nation-states with their agencies and powerful economic entities are no longer alone in space, which is increasingly accessible for others. To name one example, on February 15th, 2017, Indian space launch vehicle PSLV lifted as many as 104 satellites into orbit. Primary load was an indigenous remote sensing full-size satellite, with addition of 103 cubesats, some of them 10x10 cm in diameter. These small crafts were all operated by small and medium-size private companies and by universities. The latter were built by teams of students from United Arab Emirates [15], from Kazakhstan [1] and from Israel [3]. And the second, stunning example: the simplest commercially offered satellite comes with a price tag of 8000 USD, launch included [9].

This expanding accessibility of space systems, together with well-known capabilities to penetrate cyberspace, give malevolent non-state actors new and vast range of opportunities to negate space capabilities of states or build the ones for themselves. This situation profoundly changes the environment of space security in many ways, the most profound are following:

– outer space becomes more and more congested by entities interested in activities there;

– a number of entities that may be willing to endanger space security rises dramatically;

– forms and methods that malevolent non-state actors may employ evolve fast, from cyberintrusion into space systems, through ground-based physical interference, to launching potentially lethal constellation of nanosats;

– relations between space-faring countries may become even more complicated, as some shadowy non-state actors connected to nation-states may enter as space-faring entities.

These developments urge states to introduce some kind of technology control regime which could prevent malevolent non-state actors from obtaining potentially dangerous capabilities. Unfortunately, besides some technical co-operation within existing legal frameworks space-faring nations are unwilling to strengthen a regime of the space law.

Therefore we can expect that the developments described in this article will endure in the future and we will be confronted with increased risk for security in space. This in turn will lead to expanded range of threats and actual malicious attacks against space systems. They will therefore bring more and more costs and inconveniences for the users of Earth's orbit and their customers. The worst case scenario is triggering a Kessler effect for at least some part of the near-Earth space.

BIBLIOGRAPHY

1. Al-Farabi 1 / Gunter's Space Page, 2018 [Electronic resource] – Available from : http://space.skyrocket.de/doc_sdat/al-farabi-1.htm [Cited: 19.03.2018].

2. Ashford, Adrian R., Tytell, David. *Satellite Tracking Tool: Track the ISS, Hubble & More* / Adrian R. Ashford, David Tytell // Sky & Telescope, August 29, 2017 [Electronic resource] – Available from: http://www.skyandtelescope.com/observing/interactive-sky-watching-tools/skyandtelescope-coms-satellite-tracker/ – [Cited: 10.03.2018].

3. BGUSat / Gunter's Space Page, 2018 [Electronic resource] – Available from : http://space.skyrocket.de/doc_sdat/bgusat.htm [Cited: 19.03.2018].

4. Black, James. Our reliance on space tech means we should prepare for the worst / James Black // DefenseNews, 12 March 2018 [Electronic resource] – Available from : https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/ – [Cited: 18.03.2018].

5. CubeSat 101. Basic Concepts and Processes for First-Time CubeSat Developers / NASA, October 2017 [Electronic resource] – Available from : https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf – [Cited: 18 03 2018].

6. Dolman, Everett C. *Astropolitik* / Everett C. Dolman, – London, 2002.

7. Gleason, Gregory. *Satellite Internet and Russia's Control Over Its Cybersphere* / Gregory Gleason // Eurasia Daily Monitor Volume: 15 Issue: 36, March 8, 2018 [Electronic resource] – Available from : https://jamestown.org/program/satellite-internet-russias-control-cybersphere/ [Cited: 09.03.2018].

8. Howell, Elizabeth. *Four Cubesats Snuck into Orbit Without Regulatory Approval, FCC Says* / Elizabeth Howell // Space.com, March 16, 2018 [Electronic resource] – Available from : https://www.space.com/40001-four-cubesats-unauthorized-launch-fcc.html#?utm_source=sdc-newsletter&utm_medium=email&utm_campaign=20180317-sdc – [Cited: 18.03.2018].

9. IOS TubeSat Kits / Interorbital Systems 2018 [Electronic resource] – Available from : http://www.interorbital.com/Tubesat%20Kits – [Cited: 19.03.2018].

10. Kleiman, Matthew, McNeil, Sonia. *Red lines in Outer Space* / Matthew Kleiman, Sonia McNeil // The Space Review, March 5, 2012, [Electronic resource] – Available from : http://www.thespacereview.com/article/2038/1 - [Cited: 10. 03.2018].

11. Klotz, Irene. *Tsunami Of Smallsats Creating Opportunities And Problems* / Irene Klotz // Aviation Week & Space technology, February 28, 2018 [Electronic resource] – Available from : http://aviationweek.com/aviation-week-space-technology/tsunami-smallsats-creating-opportunities-and-problems – [Cited: 26.03.2018].

12. Livingstone, David, Lewis, Patricia. *Space, the Final Frontier for Cybersecurity?* / David Livingstone, Patricia Lewis // The Royal Institute of International Affairs, September 2016.

13. Moltz, James Clay. *Space Security and the Challenge of Collective Action* / James Clay Moltz // *Space Security Index 2014*; spacesecurity.org 2014, [Electronic resource] – Available from : http://spacesecurityindex.org/wp-content/uploads/2014/11/Space-Security-Index-2014.pdf – [Cited: 10.03.2018].

14. Nanosatellite database / nanosats.eu, January 1, 2018 [Electronic resource] – Available from : http://www.nanosats.eu/ - [Cited: 18.03.2018].

15. Nayif 1 (FUNcube 5, EO 88, OSCAR 88) / Gunter's Space Page, 2018 [Electronic resource] – Available from: http://space.skyrocket.de/doc_sdat/nayif-1.htm [Cited: 19.03.2018].

16. Phillips, Dewanne Marie. An Architecture, System Engineering, and Acquisition Approach for Space System Software Resiliency. Doctoral thesis / Dewanne Marie Phillips // The School of Engineering and Applied Science of The George Washington University, January 19, 2018 [Electronic resource] – Available from : https://scholarspace-etds.library.gwu.edu/downloads/7w62f833c?locale=en [Cited: 12.03.2018].

17. Preliminary Design of an Experimental World-Circling Spaceship. Report no. SM-11827 / Douglas Aircraft Company, Inc., May 2, 1946.

18. Space Foundation Report Reveals Global Space Economy at $329 Billion in 2016 // Space Foundation, August 3, 2017, [Electronic resource] – Available from : https://www.spacefoundation.org/news/space-foundation-report-reveals-global-space-economy-329-billion-2016 - [Cited: 14.03.2018].

19. Space Security Index 2014 / spacesecurity.org, 2014, [Electronic resource] – Available from : http://spacesecurityindex.org/wp-content/uploads/2014/11/Space-Security-Index-2014.pdf - [Cited: 10.03.2018].

20. Space Security Index 2017. Executive Summary / spacesecurity.org, May 2017, [Electronic resource] – Available from : http://spacesecurityindex.org/wp-content/uploads/2017/10/SSI-Executive-Summary-2017-online.pdf – [Cited: 11.03.2018].

21. Ziemnicki, Paweł. *GPS na celowniku hakerów. Czas na powrót radia?* / Paweł Ziemnicki // Space24, August 10, 2017 [Electronic resource] – Available from : http://www.space24.pl/gps-na-celowniku-hakerow-czas-na-powrot-radia-komentarz – [Cited: 12.03.2018].

22. Ziemnicki, Paweł. *IAI zabezpieczy platformy bojowe przed zakłóceniami sygnału GPS* / Paweł Ziemnicki // Space24, February 2, 2017 [Electronic resource] – Available from : http://www.space24.pl/iai-zabezpieczy-platformy-bojowe-przed-zakloceniami-sygnalu-gps – [Cited: 12.03.2018].

Стаття надійшла до редколегії 10.06.2018
Прийнята до друку 01.09.2018

НЕДЕРЖАВНІ АКТОРИ І БЕЗПЕКОВЕ СЕРЕДОВИЩЕ

Марек Чайковскі

Ягеллонський університет,
вул. Голебя, 24, м. Краків, Польща, 31-007, тел. +48- 12 663 10 46,
e-mail: marek.czajkowski@uj.edu.pl

Присутність людини у космічному просторі тісно пов'язана з національними та міжнародними безпеково-космічними додатками, які стали інструментом вибору для багатьох видів завдань, що виконуються військовими з початку 60-х років XX століття. Тому військове використання космосу є очевидним і загальним, але невійськові дії також впливають на міжнародну та національну безпеку. Для вирішення всіх проблем, пов'язаних з цим, був придуманий спеціальний термін «космічна безпека». Вона, загалом, посилається на всі питання безпеки, пов'язані з космічним простором.

На сьогодні розвиток космічних досліджень та експлуатації космосу характеризується постійним розповсюдженням відповідних технологій. Це стосується поширення можливостей серед зростаючого кола країн, а також недержавних суб'єктів міжнародних відносин. Таким чином, останні вже досягли здатності негативно впливати на орбітальні системи, і це швидко

зростатиме в найближчі десятиліття. Тому космічна безпека, вузько розуміється як безпека космічних антропогенних об'єктів та їхня здатність працювати безперервно, стає більш небезпечною. Цей документ посилається на одне з конкретних питань, пов'язаних з космічною безпекою, яка є недержавним суб'єктом у цій сфері. Тому ми маємо намір вивчити вплив таких акторів на питання космічної безпеки – це головна мета даної статті. Для досягнення цієї мети у статті описано аналітичну основу розуміння термінів «космічна безпека» та «недержавний суб'єкт», діяльність недержавних суб'єктів, що може призвести до збільшення загроз безпеці космосу та оцінити зв'язок між космічною безпекою та недержавними суб'єктами.

Ключові слова: міжнародна безпека; міжнародні зв'язки; космічна безпека; недержавні суб'єкти; зовнішній простір; космічна сила.