"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

DELIBERATE THREATS TO CRITICAL SPACE INFRASTRUCTURE – ASAT AND THE STRATEGIC CONTEXT

Alexandru GEORGESCU[1]
Ulpia-Elena BOTEZATU[2]
Ştefan-Ciprian ARSENI[3]
Alexandru BARBU[4]
Lidia BOIANGIU[5]

[1]Scientific Researcher, PhD Cand. EURISC Foundation, Bucharest
[2]Scientific Researcher, Romanian SpaceAgency, Bucharest
[3]Scientific Researcher,Lt. Eng., Military Equipment and Technologies Research Agency, Bucharest
sarseni@acttm.ro, 16 Aeroportuluistreet, Clinceni, Ilfov
[4]Assistant Researcher, Cpt. Eng., Military Equipment and Technologies Research Agency, Bucharest
[5]Scientific Researcher II, Eng. Military Equipment and Technologies Research Agency, Bucharest

The work was supported by a grant of the Romanian National Authority for Scientific Research, CNDI-UEFISCDI, project number 197/2012.

Abstract: *Space systems are critical enablers of a wide range of applications utilized by a global range of consumers. The provision of critical space services is vulnerable to, among other things, deliberate interruptions through anti-satellite weaponry and means. The intrinsic characteristics of space systems make them both very efficient and very hard to replace, such as limited weight, the high cost of replacement and the low number of assets. Deliberate human threats to space critical infrastructures are many, varied and highly efficient, stemming also from legitimate technologies for protection that can be modified to become efficient anti-satellite weapons. In addition to the technical details, a few issues stand out. The first is that deliberately targeting satellites lends itself to a form of MAD logic (mutually assured destruction), which limits the willingness of states to do it for fear of reprisal or being themselves affected, due to interdependencies. The second is that certain forms of anti-satellite weaponry have become accessible to non-state actors, who do not respond to traditional deterrence and for whom jamming, cyber-attacks and other forms of weaponry are cost effective and efficient means of incurring huge damage with no immediate loss of life (which is an important political consideration). The third is that vulnerability also extends to military users, whose systems should, theoretically, be better shielded, more resilient and afforded more redundancy. In practice, those systems are not enough and, in the case of the US, more than 90% of military communications are routed through civilian systems. This has given rise to interesting new approaches and insights towards US vulnerability, highlighted by a number of high profile military exercises. Now, the US military speaks of "fog of electrons", space as an Achilles' heel, critical dependence of drones and smart weaponry on space infrastructures, the equalizing effect of space system targeting on American military superiority etc. These trends are also important for other countries to note.*

Keywords*: space systems vulnerability, ASAT weaponry, deterrence logic, non-state actors, military users.*

Introduction

Directed threats against satellite systems used to be a hallmark of science fiction, however the United States ran satellite obliteration tests in the 1985 and, as recently as 2007, China used a missile to destroy the FengYun-1C meteorological satellite. Following the demonstration of Chinese technological prowess, the US replied by initiating a new round of tests, culminating in the Burnt Frost anti-satellite weapons (ASAT) test in 2008. Why are such tests so worrying and why do they provoke such strong reactions from security thinkers, military personnel and international bodies? Well, referring to the incident quoted above, the ASAT test run by China on the 750-kg Fengyun-1C at an altitude of 865 km on 11 January 2007 increased the number of monitored orbit debris by 12 per cent – as a result of this one incident, the North American Aerospace Defense Command (NORAD) has detected over 2,000 new objects the size of golf balls or larger, with the likelihood of 100,000 smaller objects, equally dangerous [11]. Dangerous to whom? To satellite systems in Earth orbit, vulnerable devices which are emerging as critical suppliers of key services to a wide range of beneficiaries?

Space systems are key enablers for a wide range of applications. This range is rapidly increasing in depth, width and quality, generating new capabilities which are integrated into new

DOI: 10.21279/1454-864X-16-I2-063

products on which both the developed and the developing world are increasingly dependent. This dependency breeds vulnerability, both to natural and man-made risks arising from the specific environment in which space systems operate, as well as to deliberate attacks seeking to destabilize societies. Space systems are vital for gathering information, coordinating global supply chains, ensuring communications, real time database synchronization for the Internet and for financial markets and many other services whose absence is unthinkable for ordinary beneficiaries, but a very real possibility from the perspective of security experts. This is why some space systems are being described as critical infrastructures, since their disruption or destruction would result in significant human and economic losses for societies, as well as in quality of life and business continuity [12].

Militaries are just one of the wide ranges of security actors taking an interest in space systems as critical infrastructures. However, they have specific competencies and the authority and resources to address categories of threats and of threatening actors that are beyond the scope of other security providers. Militaries are themselves counted among the most vulnerable users of space services, whose consumption has increased beyond the level which could have been considered safe or where certain parameters of safety could be maintained. Therefore, in order to maintain their capacity to fight, militaries are forced to explore the field of space security and, in so doing, highlight complicated issues regarding global peace, international relations, arms proliferation and strategic deterrence. The consequences of an inter-state conflict in space could be devastating, but we should also not discount the growing potential of terrorist groups and other non-state illegitimate combatants to try and impose their will by generating substantial damage and political pressure in their favour by targeting space systems. The means to do so are, after all, increasingly affordable and widespread, and the technical achievement of kinetic strike capability on the part of nation-state superpowers might prove to be less dangerous, in the end, than the ordinary tools and capabilities of a cyber mercenary targeting space systems from comfort, safety and anonymity anywhere in the world.

Space assets as military objectives

Despite efforts to prevent the development of ASAT weaponry and of space militarization, space assets are increasingly viewed as an element of military interest, both for offensive and defensive purposes. When it comes to the security of space systems, it was the spacefaring nations' militaries that first realized the emerging dependence on these systems and analyzed the security environment in which they operated and the potential for deliberate threats. Anti-satellite weaponry has been developed and deployed for testing purposes, while new capabilities are becoming increasingly feasible and cost effective.

Advanced militaries like that of the US (and Russia, and increasingly China, as well as other countries) are not just users of space services and potential developers of ASAT offensive means,but also progenitors of new applications which then enter the civilian field with great success. The most widely utilized Global Navigation Satellite System, the American GPS, became the catalyst of a wave of innovation in the private sector when the military, which operates the network of satellites, decided to improve the quality of signals to civilian users. The military still retains the authority to disrupt service even to allies in case of national emergency.

Militaries must engage in space security efforts not only to maintain and develop offensive capabilities or address their growing vulnerability to attacks on their space systems, but also in order to safeguard their countries, which are themselves registering significant dependencies.

On the other hand, this means that the modern military, in addition to possibly having its own systems, is a significant consumer of services from private operators of space infrastructures. This dependence breeds new vulnerabilities. The dependence on space systems is also inexorably bound to the ascent of cyberspace as an environment for business, politics and social interactions, as well as military operations.

A single Global Hawk drone that flies over the Middle East, consumes more transmission bandwidth than was consumed during the entire Gulf War in 1991, and 90% of the military traffic passes through civilian satellites, many with a private owner, and not through systems constructed to be resilient to various means of interrupting their functioning. Furthermore, 68% of American ammunition used in Iraq was guided through satellites, while only 10% was guided in the same manner during the Gulf War. Already, American strategists have stopped talking about the "fog of war" and have started talking about the "cloud of electrons" and about the fact that space systems are an "Achilles' heel" for the US, which is probably an apt description also for the militaries of EU countries. Military exercises even from 1990s or early 2000s, like Army After Next, Navy Global, and Air Force Global Engagement, Space Game 2, Schriever 1 and 2, or other simulations from private domain, DEADSATS, confirmed the fact that "politicians, economists and company chiefs [have] ignored the fact that space losses can affect national, economic and

DOI: 10.21279/1454-864X-16-I2-063

social security, not just in the United States, but also in the entire world".US experts concluded that even major military powers could be "taken hostage by the unknown elements of a new type of war". Another military exercise, Pacific Vision, demonstrated the vulnerability of commercial communications satellites on which they depend. Referring to China's 2007 ASAT test , General Michael Harnel from the Space and Missile Systems Centre declared that "if they take our asymmetric advantage in space, we go from an information age war machine to an industrial age war machine [...] the edge will go to the adversary" [13].

For these reasons, space systems are becoming a key military interest because of their potential impact on national security and defense, regardless of whether the military in question has the resources and knowledge to pursue an active role in space security governance.

In the United States, the US Strategic Command and, before 2002, the US Space Command, identified the "protection of space assets" as a "crucial war fighting and peacetime national objective because space products and services are integral to joint war fighting capability and an increasingly important part of national politics, economics, and culture" [17]. While the protection of space assets was the most important priority, the Space Command identified three other priorities related to it in order to achieve control of the space environment – surveillance, prevention and negation. There are more advanced paradigms for Critical Space Infrastructure Protection now, involving multiple stakeholder models and international cooperation in addition to military support, however the basic requirements for a successful program remain the same. Other requirements are also interspersed in the list below:

- Identifying and understanding threats
- Identifying interdependencies,
- Identifying third party dependencies, which carry significant and often poorly understood risks;
- Ensuring adequate sensor capacity and sensitivity;
- Ensuring adequate defensive information operation (anti-jamming, backup communication links)
- Training personnel;
- Modelling and simulation;
- Hardening and shielding system components;
- Ensuring mobility of systems;
- Developing or maintaining robust replacement capacity for offline systems [18] – in the case of the military, it can also involve maintaining obsolete systems as emergency replacements (for instance, aerial and maritime navigation aids in case the GNSS signal is down).

Deliberate threats

Critical Space Infrastructures (CSI) are subject to a wide range of threats, either man-made or natural. When discussing man-made threats, we should also consider separating them into two main categories: accidental or premeditated. Unlike the terrestrial critical infrastructures, for which special means of protection can be put in place, CSI present particular traits that must be taken into consideration before undergoing any Critical Infrastructure Protection activities. These particular traits are derived mainly from the harsh environment of CSI systems, their strategic positioning on useful orbital bands, the economic limitations that hamper space activities and the specific characteristics of various technologies. Given these traits, space infrastructure can be described as having a very challenging resilience profile, despite the fact that mankind has become dependent on their specific capabilities. Thus, the very small number of CSI systems, estimated at around 1,300 publicly known satellites [5], opens the door not just too future opportunities in economic development, but also to many possibilities of serious disruptions.

For instance, the main global navigation satellite system, namely the American GPS constellation, is formed of only 30 satellites, that are providing services for millions of users, either civilian or military, and possibly billions of beneficiaries. Yet, in recent decades multiple incipient global networks or regional ones, such as the European Galileo or Chinese Beidou constellations, have become operational with only a few assets placed in orbit, thus increasing the possibility of a catastrophic disruption of the service for a considerable amount of time. Another example is represented by weather satellites that are similarly burdened and just as important as GNSS assets.

Because of high barriers related to cost and other factors, redundancy is often too difficult to achieve for most of the space assets, while replacement is expensive and, most of all, time consuming, and while threats are diverse and omnipresent.

Deliberate human threats to space critical infrastructures are many, varied and highly efficient. Their development dates back to the beginning of the American and Russian space programs, which had an important military component and a "dual-use" philosophy regarding the development of new technologies [14]. Nowadays, many actors in the field of space develop anti-satellite systems out of legitimate technologies for protection whose fundamental capabilities allow eventual conversion into efficient anti-satellite weapons.

DOI: 10.21279/1454-864X-16-I2-063

Looking at deliberate threats against CSI systems, a considerable number of factors are present and can be activate in any time:

- The predictability of CSI trajectory;
- The orbital dynamics of CSI related to various regions of Earth, when visual contact can be possible from many regions, including ones that are considered sources for hostile elements;
- The high payoff of attacks on CSI systems, calculated as a ratio between the damage caused and the costs for an attacker to successfully fulfill its mission;
- The decreasing costs for special attacks, such as cybernetic ones that require only a computer, an Internet connection and a trained user;
- The ascension of non-state actors that do not comply with international laws, and are also not constrained from using forbidden materials or weapons.

Finally, anti-satellite attacks are the "ideal" method for inflicting substantial economic damage to a country or a region, while keeping the costs to a minimum and having zero casualties among Earths' population. Due to this characteristic and the increasing dependency of terrestrial critical infrastructures to SCI, attacks on space systems are considered to be a more efficient and effective offensive method when wanting to cripple a nations' economy. In this way, space assets have become the target of opportunity to many actors that do not wish to cause considerable casualties but do want to be taken into consideration for eventual negotiations or political projects.

A general typology of anti-satellite capabilities includes the following categories:

1) Electronic and Cybernetic attacks

Given that useful orbits are not so numerous and the majority of satellites have a reduced mobility through their architectural design, the main trajectories that satellites follow when circling the globe can be easily traced. Using these traces, an actor can launch an attack on a satellite when it passes a certain area, given that it is impossible to monitor all of the Earths' surfaces on the ground.

2) Laser attacks

Another means of crippling an operational satellite is an attack with a laser beam that can "blind" a satellite, given that optical systems installed on a reconnaissance platform are susceptible to errors, temporary or permanent malfunctions, in case a powerful beam of light is focused on them. Also, if the laser is powerful enough, it can lead to malfunctions of sensors or other equipment that are sensible to overheating [11].

3) Signal jamming

By design, satellites are controlled and managed from ground stations through dedicated communication links that are separated from the communication links that final users are utilizing. An attacker can easily manipulate these links to disrupt the communications, mainly by interfering with the ground receivers for downlinks (communication link originated from the satellite having the destination set to a ground station or user).

4) Electromagnetic pulse

Low-orbit satellites are exposed to the risk of becoming collateral losses of high-altitude nuclear explosions that generate an electromagnetic pulse (EMP) as a consequence of gamma radiations resulted during nuclear reactions. High-altitude EMPs represent a cause of concern for any country, because of their capability of permanently disrupt the functioning of not just space systems, but also of ground stations, that consist de base of critical infrastructures [19].

5) Attacks with maneuvering satellites

These distinct types of satellites are capable of approaching and even touching a targeted satellite without needing the owners' permission and, because it does not contain any explosives, it does not create any new waste. Both private and state actors are interested in developing this technology, mainly for its good use, of conducting maintenance on damaged satellites directly on the orbit, thus being able to extend the lifetime of a space asset. Yet, this scenario also allows them to become a weapon, mainly because their capacity to approach and deviate a satellite from its trajectory, causing it to malfunction or even be destroyed, but without making any space waste.

Although space is being considered as a vast place, the majority of space systems are crowded in a number of orbital bands, valuable because they pass directly above important markets or areas of scientific and military interest. This means that accidental collisions, not just with pieces of debris, but also between satellites, are possible.In February 2009, an American commercial satellite collided with a Russian military one at the speed of 11.7 km/s. Traceable debris fragments generated by the incident numbered over 2,000, with thousands more too small to trace. It was the first random accidental collision between whole satellites at hyper speeds, although there had been other incidents in the past. The Russian satellite was a 950-kg, nuclear-powered military satellite called Kosmos 225, which was launched in 1993 and deactivated in 1995. The US one weighed 560 kg, had been active since 1997, and was link number 33 in the Iridium Corporation communication network which comprised 66 units [15]. A representative from Iridium stated that the corporation received 400

DOI: 10.21279/1454-864X-16-I2-063

weekly close proximity warnings, issued when an Iridium satellite is within 5 km of another satellite, and Iridium 33 was scheduled to pass the Russian system by only 584 metres [16].

The orbital mechanics of space systems also mean that space is a very international environment. Many countries, including not only emerging ones, but also developed countries, do not have a comprehensive space program, so they directly rely on space systems that are governed by other countries or are the property of a foreign company operating under foreign laws. Furthermore, the majority of space assets and their underlining technologies are dual-use, offering services for both military and civilian users. This leads to a very complicated system of collective responsibility for maintaining inter-dependent systems, where brinkmanship and aggression can generate significant collateral damage.

The strategic context

As mentioned before, militaries were the first to pick up on the growing dependencies of their nations and of their rivals on space systems. They began to explore what this means, not just from an operational or tactical perspective, but also strategically. We have the examples of RAND Corporation reports [1] in the US or of work made public which was done by government bodies such as the Development, Concepts and Doctrine Centre (DCDC) of the Ministry of Defense of the United Kingdom [2].

They posit that mutual dependencies in space, such as states being critically reliant on each other's satellite systems, have led to a MAD (mutually assured destruction) logic that mirrors that of nuclear warfare during the Cold War. While developing new ASAT means and countermeasures, the countries are unwilling to employ them, except for testing and posturing. The fear is that an aggressive confrontation will escalate to the point of irreparably harming not just the participants, but also the entire global community. Even if the targeted system were not being utilized by the aggressor in his economy or governance system, there are still two main concerns. The first is that tertiary dependencies, through commercial partners, contractors and others would transmit the cascading disruption until it also damages the aggressor, especially in ways that could not be foreseen because of the complexity of the system-of-systems. The second is the very real possibility of retaliation, which would almost certainly be calibrated to produce maximum damage and disruption. Once a shooting war starts, even innocent bystanders from the international community will suffer and the aftermath of such a conflict, no matter how brief, is likely to be just as dangerous as the conflict itself, or even worse. Inoperative systems or fragments of destroyed space systems will litter orbital paths, indiscriminately impacting other satellite systems. The trust needed to govern space activities effectively, and assign radio frequencies or orbital bands would be severely undermined. Meanwhile, the long recovery period until new systems are put in place or old ones are repaired will cause untold economic damages, but also present severe risks if the systems in question were especially vital during national emergencies. The failure of the Japanese ALOS satellite [3], which was the main crisis and emergency situation management asset in space, took place during the Fukushima disaster, when its services were most sorely needed. Only the existence of international accords and other systems with similar capabilities in orbits favorable to monitoring Japan allowed the country's decision makers to access the required space services. When it came time to renew the system and also provide for long term study and monitoring of the Fukushima area and beyond, the Japanese took no chances and launched a constellation of satellites [4].

However, while it is true that certain ASAT capabilities are available only to the most advanced nations (laser weapons, kinetic weapons), there are also capabilities available to non-state actors and rogue nations. Moreover, these actors are generally unresponsive to considerations that responsible nation states must build their policies on, like safeguarding their economy, population, national territory, prestige and so on. Non-state actors have an especially different psychology when compared to state actors, and their rise to prominence in world affairs in general (international civil organizations, corporations, religious entities, sectorial organizations and associations) have produced significant complexity in world affairs. The non-state actors under advisement in this discussion are terrorist groups and transborder organized crime groups. The first one would have been an instinctual choice, but the second is no less deserving of inclusion. There is a very blurry line between the two groups, and organized criminal activities are an important enabler for terrorism in general, as well as in particular. In general, organized crime undermines institutions, decision makers, public morale and trust, economic activity and especially the bodies charged with states security. In particular, organized crime creates revenue streams for terrorist groups, exposes weaknesses in target institutions which may be exploited by terrorist groups, produce the means by which terrorist groups can achieve their operational goals (access to weaponry, explosive,

DOI: 10.21279/1454-864X-16-I2-063

forged identification papers or information) and can also aid them in all phases of an attack.

The proliferation of ASAT technologies, capabilities and expertise offers new opportunities to non-state actors. They might not be able to field missiles or lasers, but they are certainly capable of launching cyber-attacks, performing jamming (at ground stations especially, if not also in orbit), certain low yield laser attacks for blinding sensors and other types of ASAT interventions. Cyber-attacks, in particular, require very few resources – a laptop, an Internet connection and a person with the required skills – and can be launched from anywhere in the world.

And proliferation is an increasingly complex phenomenon. For one, proliferation of specific weapon systems is not necessary, thought it may happen, utilizing the same channels of proliferation aided by organized crime and rogue states that enable nuclear material and technology proliferation. It is just as likely that innocuous technologies and techniques could be put to use against satellite systems with enough creative thinking and calling only for generic technical expertise. The seeming legitimacy of covert preparations for ASAT strikes through such means provides perfect cover – many components for jammers or the jammers themselves can be bought off the shelf, there are plenty of books and other sources on electronics and plenty of publicly accessible information on satellite systems, helpfully collated by groups such as the Union of Concerned Scientists in one place [5].

We may find that terrorist groups could, increasingly, orientate themselves towards ASAT campaigns for strategic purposes. This could just as well become a future phase in the Global War on Terror, once a point of diminishing returns has been reached with regard to the effect of attacks with human casualties and the cost of such attacks to the organizations themselves. In contrast with classical attacks, an ASAT attack will have a high likelihood of doing significant damage for very little effort and risk on the part of the non-state actor attacker. This means that there will be a high cost to benefit ratio. Given the unpredictability (rather a dearth of simulation and modeling capacity on the part of decision makers and security experts), an attack could succeed beyond the wildest dreams of the perpetrators, either creating a cascading disruption throughout the system-of-systems compounded by the skittishness of post-crisis financial markets, or correlating (on purpose or by accident) with another negative event that will compound the initial and secondary impacts. The first example is easily illustrated by an attack that disables or degrades the GNSS positioning and navigation signals, creating havoc in very tight global supply chains with just-in-time inventories, whose effects will be immediately felt in the financial markets. The second scenario involves destroying or disabling an Earth Observation satellite which is critical to monitoring disasters areas right when its services are most needed, because of the materialization of some extreme weather phenomena, earthquake, or man-made disasters, such as nuclear meltdowns.

At the same time, these attacks can be viewed as victimless crimes, in the abstract. Government officials and security personnel will know better than to discount the threat, but it is less likely that the media and, by extension, the populations of affected countries, will react with the same visceral emotions as in the case of attacks on their soil with human casualties. This is not mere conjecture. The Irish Republican Army switched, in the 1980s, from the casualty and terror based approach to the mayhem and economic damage paradigm because of diminishing returns and the hardening of British attitudes towards their cause. The new attacks created significant damage, but all of the bombs were phoned in ahead of time to the media in order for the targeted areas to be evacuated. British rage was finally superseded by weariness of the economic costs of continuing to fight the IRA, paving the way for concessions and eventual peace. For a terrorist group with a defined agenda that is not an existential threat to the group being terrorized, such an approach could be just as rational and productive.

Of course, destruction or major disruption of targeted systems is only one option. There are others, with more insidious effects. One can steal data from remote sensing operations or communications. One can also block the transmission of certain data, temporarily inhibit information gathering or even falsify data. These are tactical operations aimed at a certain goal – pecuniary gain, preventing surveillance, inducing disruption further up the chain or infiltration. For example, simply inducing a very slight lag in the synchronization signal coming in from a GNSS system's atomic clocks can undermine the connections between the markets in the financial capitals of the world. With high frequency trading techniques being in vogue and on the cutting edge of the financial world, the attacking party can arbitrage a very small difference (on the order of nanoseconds) in the timestamps on transactions to gain significant amounts of money [6], since the same financial product on different markets will tend to converge in pricing. Or an especially destructive attacker, not interested in profit, can do on purpose what has so far only happened because of errors in trading algorithms, inducing a

DOI: 10.21279/1454-864X-16-I2-063

dynamic of trades in the market that eventually leads to a crash [7].

Another possibility presents itself, for state actors and terrorist groups alike – to utilize very specific means and finesse in control over their effects to achieve certain results while minimizing the collateral damage that would justify an aggressive counter-attack. For nation-states in particular, this is one way of skirting the edge of the MAD equilibrium in space. For instance, rather than destroy a remote sensing device that may provide incontrovertible evidence of a nuclear test being prepared [8], the state in question can temporarily blind it with a tracking lase whenever it passes above its territory, leaving the satellite fully functional the rest of the time [9].

There have been attempts to limit the militarization of space and the development and deployment of ASAT weaponry. There are formal treaties, there is the Conference on Disarmament and there are international bodies such as the UN Commission on the Peaceful Uses of Outer Space that attempt to channel a burgeoning "space race" into peaceful pursuits. But the various accords and treaties are only valid until the first state breaks them and upends the entire strategic equilibrium. Meanwhile, legitimate technological capabilities, including for security and defense, are being developed which are innately dual use and can be repurposed for offensive actions as well [10]. Technological stasis is not an option, only a continuous diplomatic rapprochement that makes clear the risks of a confrontation in space and ensures that dialogue continues to defuse potential threats to the general peace of the "orbital commons" before they manifest to everyone's detriment. Meanwhile, non-state actors are not party to any such agreements, formal or informal, do not respond to threats and deterrence the same way a responsible state actor would and are increasingly capable of ASAT operations.

CONCLUSIONS

Space systems have become critical components of wider infrastructure systems, providing important capabilities which enable advanced societies to function and prosper. They are critical enablers for a wide array of services, from information gathering and communications between individuals and systems, to command, control and coordination of the local, national and global production chains. The dependence on space systems is no longer confined to the most advanced sectors of the economies and state apparatus of the most advanced nation, but is increasingly occurring in developing economies, whose path to prosperity and economic, social and political catch-up involves an increasing reliance on the provision of critical space services. Being a spacefaring nation is no longer a precondition for utilizing and becoming dependent on space systems. However, these critical systems face numerous and daunting threats, as well as difficulties in ensuring resilience and risk governance. One of the most important threats is the development of anti-satellite weapon systems, which exhibit significant variation in cost, complexity and means of action.

Alongside other threats, ASAT weapons force us to consider the frightening possibility of a disruption in the supply of critical space services that would cascade throughout the infrastructure system-of-systems, generating significant damage which will not be confined on one side of a political border, but will reverberate globally. Only the lack of a damaging event so far has served to obscure the significant vulnerability of our dependence on vulnerable space systems. It would take just one very damaging attack with very heavy media attention for this to become one of the main reasons for concern and to induce a mentality of uncertainty that can derail investor and consumer confidence.

With so much at stake and so many interconnections in play, nation-states are increasingly unlikely to utilize attacks on space systems, for fear of either damaging themselves or inviting a devastating retaliation. A state which is advanced enough to field ASAT weaponry is advanced enough to be very vulnerable to counter-attack along those same lines. While deterrence can fail and countries may engage in brinkmanship regarding the testing and use of ASAT weapons, it is not they who are the principal concern, but the rogue states and the non-state actors (terrorist groups, transborder organized crime groups). These entities, especially the latter ones, do not respond to the usual logic of deterrence, but they are increasingly likely to own ASAT capabilities of their own, either through the proliferation of technology or weapon systems, or through the development of accessible means, such as cyber-attacks and jamming, to affect the functioning of space systems.

The solutions, so far, are minimal and mostly defensive/passive in nature. The first is to harden space systems (shielding, cyber protection, redundancies, extra capacity, and substitutions) or reduce the dependency of critical infrastructure systems on them. The second is to affect the behavior of actors capable of threatening the functioning or integrity of space systems. In the case of state actors, one can deter the use of ASAT weaponry, or establish a better framework to underline a common dependence on space to prevent militarization and conflict there. Things are more complicated with non-state actors. With regard to anti-proliferation efforts, one only has to fail once for the efforts to be severely compromised. Since one cannot actively pursue and thwart unknown threats, states are reduced to a defensive posture, where they must

DOI: 10.21279/1454-864X-16-I2-063

mitigate the effects of attacks and cooperate to eliminate any threats as soon as they are identified. This is harder to achieve than it sounds, since there is a conflict between need-to-know and need-to-share when it comes to cooperation on international security even among formal longtime allies, like NATO, let alone between potential rivals in every other area except collective security.

These issues should also be a concern also for the authorities in countries like Romania, which are not spacefaring nations, but are critically dependent on space systems for their continuing development. At the same time, countries like Romania face categories of political and economic risk related to their dependence on systems owned by foreign companies, under the sovereignty of other states, which must comply with national security legislation or regulations governing dual use systems and technologies. There is not much practical difference between an attack that degrades a system's capacity, such as its accuracy for positioning, and the invocation by military authorities of a national emergency in order to limit the quality and supply of service for non-favored or civilian users. It is true that the crisis moment may pass more quickly in the second scenario, but the practical effects are the same.

Ultimately, the private owners/operators/administrators of space systems must also come to grips with the new security landscape and its increasing uncertainties. And they must also be ready to work within a framework with state, academic, private and civil society actors in order to perform risk governance from an all-hazards approach perspective. If governments fail to make these responsibilities clear and coopt and incentivize private actors to be more security conscious, then the resilience of nations will be under threat because in space, just as on the ground, private entities own more and more of the critical infrastructures on which we depend (60-80% of terrestrial infrastructures).

BIBLIOGRAPHY

[1] A. Long,"Deterrence – From Cold War to Long War", RAND Corporation, 2008.Available at: http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf.

[2] Ministry of Defence (MoD), "Space: Dependencies, Vulnerabilities and Threats", Development, Concepts and Doctrine Centre (DCDC), Shrivenham, 2012, section 4-8.

[3] T.Iwasa, "Disaster monitoring activities in Japan", Office for Space Utilization Promotion of the Ministry of Education, Culture, Sports, Science and Technology of Japan (MEXT), presentation given to the United Nations Office for Outer Space Affairs, February, 2012. Available at: http://www.unoosa.org/pdf/pres/stsc2012/tech-11E.pdf.

[4] S. Yoshimoto et al., "Environment Monitoring of Fukushima and Chernobyl Areas using a Constellation of Earth Observation Microsatellites", University of Tokyo, as part of "Japan-Ukraine Cooperation Technical Demonstration Program for Supporting Aftermath Responses to Accidents at Nuclear Power Stations", November 20, 2013. Available at: http://www.nanosat.jp/images/report/pdf/NSS-05-0104.pdf.

[5] Union of Concerned Scientists open-source satellite database statistics. Data available at: http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB.

[6] Humphreys, Ledvina, Kintner, Psiaki, O'Hanlon, „Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer". Available at: http://gps.mae.cornell.edu//humphreys_etal_iongnss2008.pdf.

[7] Kirilenko, Kyle, Samadi, Tuzun, „The Flash Crash: The Impact of High Frequency Trading on an Electronic Market", October 2010. Available at:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1686004.

[8] BhupendraJasani, "Chapter 12. Role of Satellites in Strengthening Nuclear Security". Available at: https://www.mcgill.ca/iasl/files/iasl/wef-mcgill_space-jasani.docx.

[9] V. Gupta, F.Pabian, "Viewpoint: commercial satellite imagery and the ctbt verification process". Available at: http://cns.miis.edu/npr/pdfs/gupta53.pdf.

[10] A. Gheorghe, D.Vamanu, "Risk and Vulnerability Games: The anti-satellite weaponry", 2007, Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, pp. 457–470.

[11] Carmen Pardini and Luciano Anselmo, "Evolution of the Debris Cloud Generated by the FengYun-1C Fragmentation Event", Space Flight Dynamics Laboratory, Istituto di Scienza e Tecnologiedell'Informazione Alessandro Faedo, Pisa, Italy, 2007. Available at: http://issfd.org/ISSFD_2007/10-4.pdf, accessed 20 April 2016

[12] Moteff J., Copeland C., Fischer J., "2003 Critical Infrastructures: What Makes an Infrastructure Critical?" Report to Congress, Washington DC.

[13] Ian Easton, "The Great Game in Space - China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy", published by Project 2049 Institute, p. 8. Available at: https://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf.

[14] Laura Grego, "A History of Anti-Satellite Programs", pg. 10, Union of Concerned Scientists Global Security Program, January 2012. Available at: http://www.ucsusa.org/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

DOI: 10.21279/1454-864X-16-I2-063

[15] Brian Weeden, "Billiards in Space", Space Review, 23 February 2009. Available at: http://www.thespacereview.com/article/1314/1, accessed 20 April 2016.
[16] T.S. Kelso, "Iridium 33/Cosmos 2251 Collision", 15 July 2009, Center for Space Standards and Innovation, Colorado Springs, USA. Available at: http://celestrak.com/events/collision.asp.
[17] "Protection of space assets", Section XIV, page 2, US Space Command, 2001.
[18] "Space: Dependencies, Vulnerabilities and Threats", section 4-14, Centre for Developments, Concepts and Doctrine, United Kingdom Ministry of Defense, 2012.
[19] William Graham et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack", Critical National Infrastructure Series, April 2008, ISBN 978-0-16-080927-9.

DOI: 10.21279/1454-864X-16-I2-063