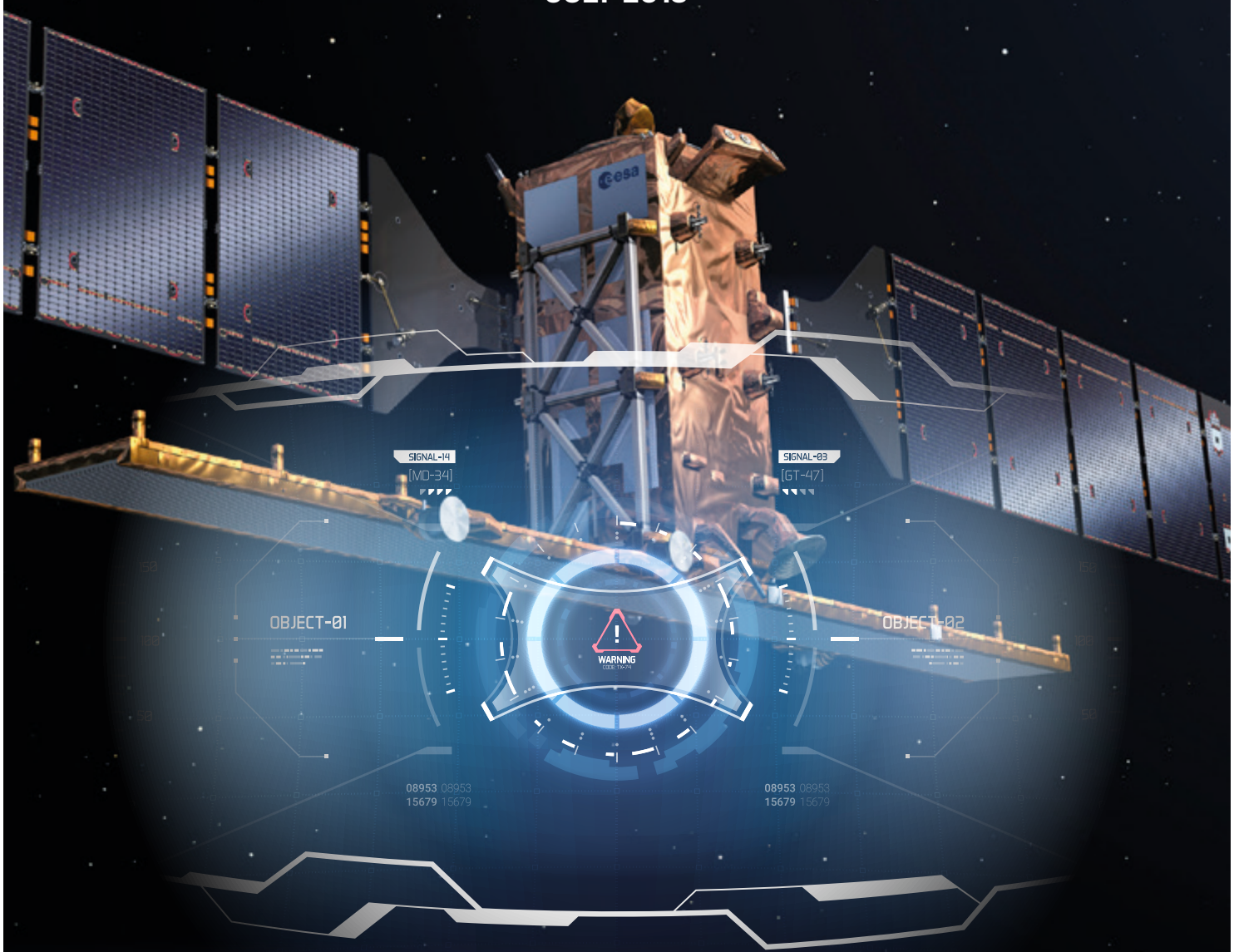
EUROPE'S PREPAREDNESS TO RESPOND TO SPACE HYBRID OPERATIONS

PSSI REPORT

JULY 2018



Prague Security Studies Institute

Contents

I. Background and Rationale

Hybrid operations in space are not a new phenomenon. To date, however, issues related to these operations have largely been confined to classified, often stove-piped, environments. Open discussions concerning hybrid threats have been almost exclusively focused on the terrestrial and maritime domains.

Europe's competitors have become fond of operating in the "grey zone", an environment that permits them to achieve desired objectives or effects without triggering unwanted military or political response by other nations. Examples include, Russia's activities in Crimea and the Black Sea and their global information operations,[1] China's illegal island building/militarization in the South China Sea and its cyber campaigns in Europe and U.S., and Chinese and Russian economic and financial (E&F) "nation-capturing" activities.

Given the advances in counterspace capabilities of an increasing number of states, especially China and Russia, coupled with a far more contested space domain, these activities are of growing concern. It is not only military, but also civil and commercial space capabilities that are now at greater risk.

In 2016, General Joseph Dunford, the U.S. Chairman of the Joint Chiefs of Staff, stated that U.S. adversaries compete "with a military dimension short of a Phase 3 or traditional conflict".[2] In January 2018, France's Joint Space Commander, Air Force General Jean-Pascal Breton, observed that the space environment is being contested in new ways and that it is essential to have the capability to detect and identify potential unfriendly or aggressive acts.[3]

Increasingly, military and civil policy decision-makers will be confronted with this harsh reality and will be in need of a comprehensive assessment of these threats and available solution sets.

To bolster a discussion in Europe concerning this family of issues, the Prague Security Studies Institute (PSSI) convened, on May 18, 2018, in Prague, a roundtable on this topic, entitled "Responding to Unconventional Threats to Europe's Space Operations" (see Annex 1). The participants included senior governmental and non-governmental space experts from 12 countries (see Annex 2).

The roundtable had three primary goals. First, establish a framework for an unclassified discussion concerning space hybrid operations and their knock-on effects, and a stock-taking of some of the more obvious examples. Second, configure key arguments for European civilian, military and commercial decision-makers to raise the priority of these threats within their respective countries. Third, review potential options available in Europe to help integrate these threats into the security architectures of individual NATO and EU member states with the aim of strengthening space infrastructure resiliency, deterrence, and quick, effective responses. This roundtable helped inform and shape the content of this report.

II. Bottom-Lines

Competition in space to gain a strategic advantage on Earth has been with us since the dawn of the space age. Today, the global counterspace dynamic is driven by the U.S. – China – Russia rivalries, accompanied by other factors, such as a surge of new space actors (including commercial) and advancement and proliferation of space technology. As a recent Mitchell Institute for Aerospace Studies policy paper put it, space actors globally are "participants in a fundamental reordering of many tenets and assumptions" nationally and internationally.[4]

The combination of reliance on space for military operations and immensely important socio-economic services to our nations, and an increasingly active concern about maintaining space stability to manage geopolitical flashpoints (e.g., North Korean nuclear brinkmanship, Iranian proxy conflicts and direct engagements in the Middle East etc.), have spotlighted space vulnerabilities as never before.

Competitors and adversaries are less clearly delineated than during the Cold War and threats to space operations are becoming more diversified, driven by technological progress and innovations, as well as by the appetite of the most capable authoritarian regimes to assume an ever-greater global role. In short, terrestrial disputes are at risk of crashing over traditional boundaries into space in the near-term. European space policy-makers are almost out of time to prepare adequate contingency plans.

Without doubt, more unintended threats to space, such as space debris and radio frequency interference will – and should – continue to receive priority attention. That said, the proliferation of innovative technologies, such as small satellites or so-called "mega-constellations" (structures of several hundred satellites deployed in low-Earth orbit),[a] the dual-use features of active debris removal (ADR), menacing rendezvous and proximity operations (RPO), as well as new actors (many of them commercial), will require enhanced Space Situational Awareness, and eventually a comprehensive Space Traffic Management (STM) regime.

Figure 1: Today, constellations can be less expensive, weighing as little as 1 kg and can be comprised of hundreds of satellites. (credit: SatMagazine)

ADR systems are a good example of how space assets can be utilized for both, benign and aggressive actions. These systems are purposed to remove a dysfunctional space object by using another spacecraft. That, however, means that they can also be used for removal of, or interference with, a functional system. Active satellites often lack sufficient defense mechanisms and can be rather easily compromised.[5] Various systems involving, for example, space tugs or lasers have been proposed as ADR.[6] RPO activities are tightly connected to some ADR methods. RPOs can be used both for civil missions (e.g. ESA's CleanSpace One mission aiming to demonstrate ADR technologies and de-orbit the SwissCube satellite), but also for far less transparent, offensive activities targeting another country's satellites.[7]

Figure 2: In 2016, China launched Aolong-1, 'The Roaming Dragon,' one of four small satellites sent into orbit aboard the Long March 7 rocket. According to the Harbin Institute of Technology, the satellite was sent to complete a demonstration of space debris mitigation technology by using a small robotic arm to capture debris pieces and launch them toward the atmosphere. (Credit: Xinhua)

a Some 2,400 small satellites of 1-50 kg are expected to be launched until 2023. The company LeoSat (a partner of Sky Perfect JSAT), for example, plans to have a full constellation of 108 satellites placed in orbit by 2022. Other companies that announced plans to launch mega-constellations include Iridium, SpaceX, and OneWeb. Besides the difficulty connected with their tracking, characterization, and continued presence in orbit after their short lifetime, there is also a possibility of these capabilities being used for nefarious purposes. (source: Vedda, J. & Hays, P. (2017). 'Major Policy Issues in Evolving Global Space Operations,' *Mitchell Institute*, (Policy Paper Vol.9, p.9), Available at: http://www.airforcemag.com/DRArchive/Documents/2017/120517_MitchellPolicyPapers_SpaceOperations.pdf, (December 2017); and LeoSat. Available at: http://leosat.com/media/1114/leosat-technical-overview.pdf.

There is a worrying "grey zone" spectrum of threats associated with deliberate actions that are potentially of great concern due to their asymmetry and possible strategic effects. PSSI defines space hybrid operations as "*intentional, temporary, mostly reversible, and often harmful space actions/activities specifically designed to exploit the links to other domains and conducted just below the threshold of requiring meaningful military or political retaliatory responses*".

These malevolent activities can take a variety of forms, including directed energy operations, electronic operations, cyberattacks, RPOs, or economic and financial initiatives that are aimed at partial or full control of the space sectors of various nations (so-called "space sector capture").[8] Table 1 below illustrates select examples of space hybrid operations that could be deployed.

SPACE HYBRID OPERATION[a]	EXAMPLES	ATTRIBUTION	REVERSIBILITY
Directed Energy Operations that May Result in Space Debris[b]	Low-Power Laser Dazzling or Blinding[c] High-Power Microwave (HPM) or Ultrawideband (UWB) Emitters	Varies	Generally Reversible
Orbital Operations that Generally Do Not Result in Space Debris	Space Object Tracking and Identification; Rendezvous and Proximity Operations (RPO)	Varies	Fully Reversible
Electronic Operations[d]	Jamming[e] (Orbital/Uplink, Terrestrial/Downlink) Spoofing[f]	Moderate	Fully Reversible
Cyber Operations[g]	Attack on satellite or ground station antennas Attack on ground stations connected to terrestrial networks Attack on user terminals that connect to satellites	Difficult	Generally Reversible
Economic and Financial (E&F) Operations[h]	Investments in targeted country's space infrastructure for purpose of influence/control Provision of loans and construction/launch of targeted country's space system(s)	Varies	Generally Reversible

Table 1: Illustrations of Deployable Space Hybrid Operations[9]

In 2006, China exercised its capability to blind a U.S. surveillance satellite. In 2014, China hacked the U.S. weather satellite system.[10] During the annexation of Crimea, Moscow jammed communications and spoofed GPS systems. In 2015, a Russian military satellite made several close maneuvers in a vicinity of two Intelsat satellites in geostationary orbit (reportedly one of the first publicly noted incidents of a commercial operator being approached by a foreign military satellite). Last year, Russia reactivated its satellite, Kosmos 2504, launched in 2015, and conducted maneuvers close to the remnant of a weather satellite shot down by China in 2007. In December 2017, French Joint Space Commander, Gen. Jean-Pascal Breton, admitted that his country's satellites have been closely inspected by foreign governments.[11] A similar remark was made by his predecessor, General Jean-Daniel Teste, in 2016.[12]

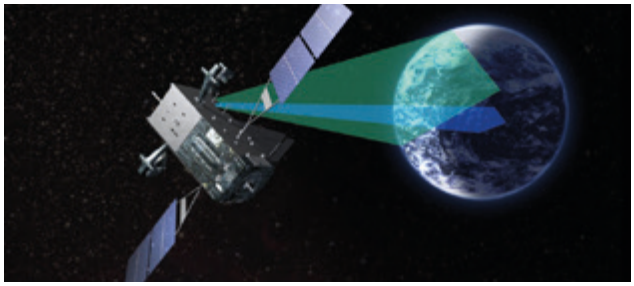


Figure 3: High value, strategic space assets, such as U.S. military's Space Based Infrared System (SBIRS) are now potentially vulnerable. (Credit: Lockheed Martin)

a This list purposely does not include ground-based kinetic ASAT weapons, co-orbital kinetic weapons, electromagnetic pulse (EMP) weapons, high-power lasers, etc. as their effects are easier to attribute and are not reversible.

b The attack is swift and degradation of the targeted spacecraft may not be immediately apparent.

c Spoofs or jams of satellite electro-optical sensors using laser radiation that is in the sensor pass band (in-band), temporarily blinding the satellite.

d The use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack an adversary's space system. Communications/navigation satellites and other satellite's communications, data and command links are likely targets.

e Emitting noise or some other signal for the purpose of preventing the sensor from being able to collect the real signals.

f Emitting false signals that mimic real signals to cover the real signals (a type of electronic decoy).

g Targets data and the systems that use the data (i.e. information services and operator's control over the asset).

h Use of economic and financial transactions to advance "space sector capture" (PSSI defines space sector capture as "a state actor's provision of space-related equipment, technology, services and financing ultimately designed to limit the freedom of action and independence of the recipient state's space sector, generally implemented on an incremental basis").

A well-known example of cyber-espionage using space assets was undertaken by the Russian-led Turla group, which hacked into satellites to gain access to sensitive and confidential information of Western embassies, government institutions, and military entities between 2008 and 2016.[13] The attack was used against forty-two countries, including the United States (U.S.) and six European States (France, Germany, Latvia, Poland, Serbia, and Spain).[14]

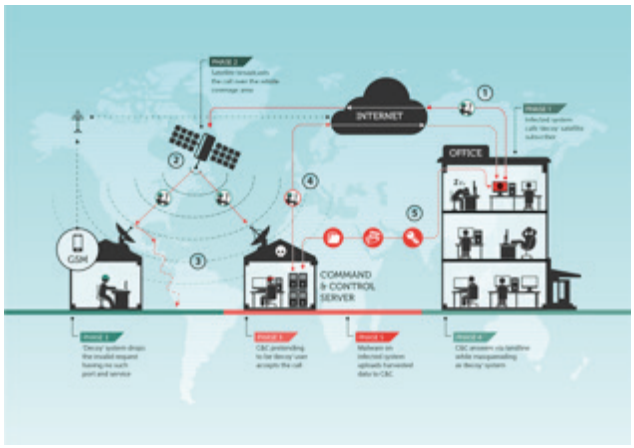


Figure 4: Attacks on satellite-based Internet connections, as conducted by the Turla group between 2008 and 2016, are a cheap and efficient way to compromise foreign networks or cover illegal activities. (Credit: Kaspersky Lab)

E&F operations involve the use of economic and financial incentives to targeted countries, most often through state-owned enterprises (SOEs), to accomplish "space sector capture". PSSI defines space sector capture as "a state actor's provision of space-related equipment, technology, services and financing ultimately designed to limit the freedom of action and independence of the recipient state's space sector, generally implemented on an incremental basis". These transactions, including subsidized financing and below-market terms and conditions, are also employed to expand an authoritarian space actor's global space footprint (with a number of accompanying benefits). Countries lacking a space program, funding, and technical expertise are generally open to, for example such Chinese and Russian offers, even if it means their countries will become perilously dependent on these outside benefactors.[15]

In Africa, for example, Russia launched a satellite for Egypt in 2014 and is assisting in the development of their second satellite to be launched in 2019.[16] Ethiopia plans to develop its own space launch vehicle and satellites,[17] and Russia, which earlier this year wrote-off $162 million of Ethiopia's debt, has agreed to assist in engineering, science and technology likely to involve its fledgling space sector.[18]

Russia has also "assisted" South Africa, which established its own Space Agency in 2010, in developing a satellite surveillance program.[19] Back in 2007, China helped Nigeria build and launch a commercial satellite (the first time China had reached out to a foreign country in this fashion), followed up with the launch of a communications satellite in 2011, and has discussed the possibility of sending the country's astronaut to space in 2030s.[20]

In South America, China Harbour Engineering Company (CHEC), a subsidiary of PLA-affiliated China Communications Construction company, built a satellite tracking, telemetry, and command station in the Patagonia region of Argentina, based on an agreement between China Satellite Launch & Tracking Control General (CLTC) and Argentina's Comisión Nacional de Actividades Espaciales (CONAE). (CHEC is also involved in illegal island-building, and militarization of same, in the South China Sea). This Chinese facility, their first of this scale abroad, became operational in April 2017.[21] Such transactions advance the strategic objectives of countries like China and Russia, that seek to eventually leverage undue dependencies without the worries of negative media attention, security-minded due diligence, or elevated market risk.

Common characteristics of hybrid space operations is that they often involve ambiguous attribution, temporary and reversible effects, and are generally not visible publicly. Space is, by nature, a critical domain for hybrid operations and warfare. In that sense, it is no different from land, air, sea, and cyberspace. Some of the key issues embodied in space hybrid operations are listed in Table 2 below:

Temporary/Reversible Nature	deployment of capabilities that disrupt or deny space-derived benefits for a specific period of time
Attribution	due to limitations in existing SSA capabilities, it is often difficult, if not impossible, to clearly attribute space hybrid operations
Verification	enhanced intelligence-sharing and SSA capabilities required (arms control techniques are generally not workable in space)
Enforcement of Norms	what is known and measurable (ideally by several governments) should be enforceable
Deterrence	increase consideration of options outside the space domain, as reactions within it carry severe downside risks
E&F Cross-Domain Deterrence	E&F deterrence and responses to space transgressions are particularly attractive, as they can damage the offending state in the legitimate international trading and financial systems via elevating risk profiles, harming reputations/brands and other means

Table 2: Key Issues Embodied in Space Hybrid Operations

Due to the asymmetry of vulnerabilities and effects (embodying significant escalatory potential) for all space actors (i.e. military, civil and commercial), and the lack of precedents, the consequences of actual incidents are difficult to predict. Space hybrid operations should be thought of as a number of events, rather than a single incident, that probe the gaps in preparedness, readiness, allied coordination and response options of a competitor/adversary. Better understanding these capability gaps permits an adversary to configure an effective strategy to gain a decisive advantage.

Accordingly, how to operate in a contested, degraded and operationally-limited space environment becomes essential. Resiliency includes, besides technical solutions, sound policy and strategy related to protection of critical infrastructure. Various measures are described in a 2015 Pentagon report entitled "Space Domain Mission Assurance: A Resilience Taxonomy", with an emphasis on deception, disaggregation, distribution, diversification, proliferation and protection.[22] Not only does resilience requires partnerships among allied nations, but also usable links with other partners, and even competitors, to deter these low-intensity, hostile operations.[a]

Deterrence against lower threshold attacks, which could potentially lead to far-reaching disruption, would ideally be configured in a domain other than space and by non-military means (as "mirroring" an attack is generally not a viable option due to undesirable consequences with regard to our utter dependency on space). Lack of certainty over whether an attack has happened, where it originated and what the attacker is trying to achieve all make a proportional response more difficult.[23]

Cross-domain response options are designed to dissuade an adversary from seeking to deliver asymmetric effects via space or penalize the perpetrator convincingly. In this context, economic and financial (E&F) means can make a clear distinction between countries that respect free and fair market principles and state-led economies that often show little regard for these principles. Tracking and mapping the international transactions of state-controlled companies in global space sectors reveals what these countries are doing, as opposed to what they are saying, which are frequently at odds.[24]

The network of subsidiaries of these enterprises help them blur their identities and confuse the "risk management" and compliance side of the markets. As the global markets are sensitive to financial risk-related information, publically identifying companies (particularly those that are publically-traded) engaged in malevolent space-related activities would be one element of a package of such measures designed to deter hostile behavior in space (i.e. putting at risk acceptance in, and unfettered access to, the international trading and financial systems or various power projection initiatives[b]).[25]

a With regard to positioning, navigation, timing (PNT) services, for example, the U.S. and Europe are seeking to ensure, through agreements, that GPS and Galileo are compatible and interoperable, providing a fallback for either service if the other is malfunctioning or becomes a victim of a "bad actor" attack.

b E.g. China's "Belt and Road" Initiative.

III. Key Findings

The main findings of the report are: asymmetric space vulnerabilities are a critical security issue in the broadest sense; a greater effort is required to work toward dynamic Space Domain Awareness (SDA) capabilities; space should be included in the treatment of hybrid threats; and space partnerships are essential to strengthen deterrence against these threats.

Reality of Asymmetric Space Vulnerabilities

The roundtable reconfirmed that space assets have become more vulnerable to being compromised by Europe's competitors and adversaries. The roundtable participants agreed that there is an urgent need to protect space infrastructure from variety of risks and threats. This is due, in large part, to the fact that European countries are now critically dependent on space assets and which are expected to deliver an ever-growing menu of economic, social, security, and defense-related services.

A PwC study asserted that in 2016 some 7% of the European Union's (EU) Gross Domestic Product (GDP) depended on space infrastructure. The European Commission (EC) estimated in its recent Commission Staff Working Document that benefits derived from the European GNSS will amount to between € 55 billion and € 63 billion over the next 20 years, most of which will come from downstream industrial development.[26] The benefits derived from the EU's Earth Observation system, Copernicus, between 2017 and 2035 is estimated to amount to between € 67 billion and €131 billion.[27] It is projected to enable more than € 13,5 billion of cumulative economic benefits in gross value added by 2020.[28]

London Economics (LE), a UK consulting firm, stated in its June 2017 report that most industries in the United Kingdom (UK) depend, to some extent, on GNSS. LE tried to assess how costly it would be if GNSS was unavailable for five days.[a] The overall loss was measured to be £5.2 billion (which is some € 5.8 billion or $6.8 billion). The scenario considered impacts on widely used infrastructure (e.g. transport, etc.) and various fields, such as defense, energy, finance, food supply, etc.[29]

Knock-on effect would probably kick in quite rapidly. Without global GNSS, communications and Earth observation services, bank transfers would be interrupted, the exact time (determined by satellites) would be unknown, some internet connectivity would be unavailable and traffic management and infrastructure would collapse.

In only a few hours, economic, education, healthcare, communication and transportation challenges would be impacted. Military operations and, thus, national security, would be put at risk. Moreover, a cascading effect would emerge. Agriculture and resource management would be cut off from essential data. Loss of remote sensing would deepen the tragedy of disasters. Although the final consequences are difficult to predict, without doubt, the loss of satellites would have a destructive impact on everyday life.[30]

Figure 5: Space assets are vulnerable to attacks. (An artist image of a laser weapon. Credit: Getty Images)

It is probably fair to say that there are not many effective tools currently available in Europe to prevent, and manage, these grey zone threats. The lack of visibility of an attack, difficulty in identifying its source and intent, as well as its temporary and reversible nature, often make them seemingly fragmented occurrences with no easy deterrence solution or response.

Various European space actors emphasize different dimensions of space security. The European Space Agency (ESA) covers space security under its "space safety"-related activities. The EU also covers (as a

a Five days is the general input for scenarios as they are approached by the National Risk Assessment (NRA) for critical infrastructure.

necessity) various "space security" challenges. NATO, at its recent summit in Brussels, announced the development of an overarching NATO space policy that would include a "Space Support to Operations" component.[31]

Individual programmatic decisions, such as optical secure telecommunications developed by the European Space Agency, are being implemented, that seek to deal with not only safety issues (such as crowded radiofrequency spectrum[a]) but also security issues, in this case cyber threats feature most prominently.

That said, telecommunication links in the frequency bands above 3000 GHz, with the ability to support data rates in the tens of Gbit/s (resulting from technological developments in optical communication devices such as optical fibre, solid state lasers (GaAs, InP)1, modulators (electro-optic modulators) and detectors (photodiodes),[32] are not, for example, currently allocated to any radio communication service or protected by the International Telecommunications Union (ITU) Radio Regulations.[b]

Working Toward Space Domain Awareness (SDA)

Situational awareness and continuous analysis of space hybrid operations is critical. The dual-use potential of space technologies establishes a thin line between a benign and an offensive action. Accordingly, even announced and seemingly inconspicuous actions could be turned into offensive operations. A mapping and tracking capability that would help identify, and monitor, such incidents will be required to determine what is an isolated event or a part of a hybrid campaign.

Such a capability would have to integrate information from other areas (e.g. legal constraints on response options, possible economic impacts, etc.). Without considerable information concerning the context of emerging threats, an appropriate response would be difficult to configure. Accordingly, it is desirable to work toward comprehensive Space Domain Awareness (SDA).[c]

Space Situational Awareness (SSA) helps characterize objects, identify their owners, infer their capabilities, calculate their future trajectories and decipher their intent, thus providing crucial information on which to base deliberations and actions.[33]

Today, European countries collaborate on enhancing SSA through the EU's Space Surveillance and Tracking (SST) Support Framework Program and a related consortium of Member States. The Consortium consists of five European member states which are represented through their national entities: France (CNES), Germany (DLR), Italy (ASI), Spain (CDTI), and United Kingdom (UKSA).[34] Its model of governance takes into account both civil and military dimensions, respects the sovereignty of individual EU Member States, and does not threaten bilateral or other arrangements that the Member States might have concluded.[d]

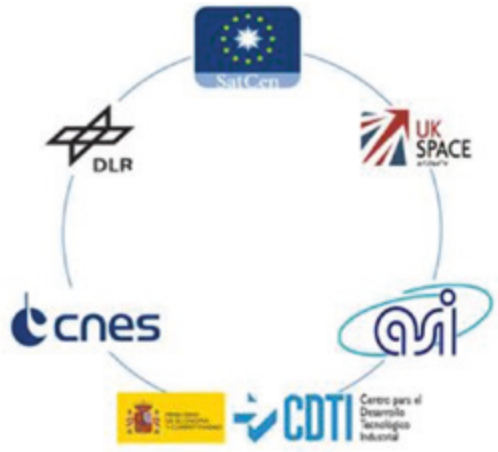


Figure 6: The SST Consortium, cooperating with the EU SatCen, is composed of five EU Member States which are represented through their national designated entities: France (CNES), Germany (DLR), Italy (ASI), Spain (CDTI) and United Kingdom (UKSA).

a In ITU's Radio Regulations Article 4.10 "Member States recognize that the safety aspects of radionavigation and other safety services require special measures to ensure their freedom from harmful interference". Harmful interference is defined as an "interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations (RR1.166 to RR1.169).

b See Article 5 of the ITU Radio Regulations.

c Space Domain Awareness (SDA) is defined as actionable knowledge required to predict, avoid, deter, operate through, recover from, and/or attribute cause to the loss and/or degradation of space capabilities and services. (source: M. J. Holzinger and M. K. Jah. "Challenges and Potential in Space Domain Awareness", Journal of Guidance, Control, and Dynamics, Vol. 41, No. 1 (2018), pp. 15-18. https://doi.org/10.2514/1.G003483)

d The EU itself is not part of this Consortium.

With regard to operations, the three initial services (i.e. collision avoidance, re-entry, and fragmentation) have been provided 24/7 since July 1, 2016 to European institutional users and spacecraft owners/operators through the EU SST portal under the responsibility of the EU Satellite Center (SatCen). They, in turn, rely on U.S. data primarily provided by JSpOC and currently operational national sensors of the EU SST Consortium members and Austria, Poland, Portugal and Romania.[35] As of April 2018, there were 35 user organizations covering 111 registered spacecraft (56 in GEO and 46 in LEO).[36]

The report from the European Commission to the European Parliament and the Council on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-2017) published in May 2018 estimated the following level of coverage for various sizes of object according to different orbital regimes.[37] It compared the performance of the initial architecture in 2017 with that expected in 2021 after the upgrades:

	2017 (initial architecture)		2021 (expected architecture)	
MS architecture (orbit and object size)	Total observed (%)*	Total well observed (% of the total) **	Total observed (%)*	Total well observed (% of the total)**
LEO (> 7 cm)	19%	14%	35%	19%
LEO (> 50 cm)	79%	72%	95%	80%
LEO (> 1 m)	96%	95%	98%	97%
MEO (> 40 cm)	18%	7%	62%	7%
GEO (> 50 cm)	40%	30%	66%	42%

* *Observed objects are objects that were observed at least once during the 14-day period of the simulation.*

** *Well-observed objects are those observed objects that were observed every day in LEO and every three days in MEO/GEO*

Figure 7: Estimated level of coverage by size of object and orbit of the initial architecture (2017) and expected architecture (2021).[38]

Decision 541/2014/EU, establishing the SST Support Framework, acknowledges the sensitive nature of SSA, leaving the operation of sensors, the processing of data, and the national SST assets under the authority of the participating Member States. The stated political objective is an appropriate and acceptable level of autonomy. Accordingly, it seeks to find complementarities with the U.S. Space Surveillance Network, rather than replicate its capabilities.

European countries are currently identifying different architectures for the future (including sensors in new geographic locations). The European Commission proposes a more Europe-wide approach and argues that future SSA requires less dependence on the United States, an EU label, and improved governance and funding.[39] Regardless whether SSA will become one of the future "flagship programs" for the EU, it is an important platform for including space hybrid threat assessments.

NATO, as a military alliance dependent on space assets (e.g. SATCOM, ISR, integrated tactical warning and attack assessment, weather information, Position, Navigation and Timing, etc.)[40], is exposed to space-related threats.[41] NATO is aware that the maintenance and security of space-based systems are critical for the Alliance.[42] Accordingly, it acknowledges the importance of SSA, which it defines as "the knowledge and the understanding of military and non-military events, activities, circumstances and conditions within and associated with the space environment or space-related systems that are relevant for current and future NATO interest, operations and exercises".[43] Any effort aimed at developing effective multinational SST networks to enhance SSA, like the European SST project, is welcomed by NATO.[44]

In addition, comprehensive Space Domain Awareness (SDA) was established as a foundational element enabling the achievement of the NATO Long Term Aspect (LTA) for NATO Space Capability Preservation.[a] In 2018, NATO launched the "Collaborative Space Domain Awareness Data Collection and Fusion Experiment", under its Science and Technology Organization (STO). The objective of this activity is to conduct a mutually agreed-upon activity that involves the collaborative collection and exchange of space domain awareness data and information.

There is no precise scope of what constitutes SDA data, but STO considers its basic elements to be "space weather and environment reporting, space object tracking and orbit characterization, space object collision and avoidance warning, radio frequency interference characterization and attribution against satellite control links and communication services".[45] The

a The Long Term Aspect (LTA) for Space Capability Preservation was established by NATO Atlantic Command Transformation to stimulate development of cross-NATO technical and non-technical solutions leading to improved survivability and availability of NATO-critical space functionality. The Systems Concept and Integration (SCI) Panel (at SCI-238 Specialist Meeting in March 2013) confirmed that NATO is significantly dependent on space services to conduct military missions and related responsibilities. It also acknowledged gaps in contingency capabilities and shortcomings in the resiliency of NATO's access to, and use of, space services. At 2015 SCI-268 Specialist Meeting, NATO STO created the basis for promoting a shared awareness for NATO space resiliency as well as identifying the most appropriate technical investments to be considered by NATO.

working group will manage and direct the collection and exchange of SDA data within the participating member nations. This initial experiment is to address elementary capabilities with the prospect of broadening the scope in the future.[46]

SCOPE

– Foundational elements of an effective Space Situational awareness (SSA) environment;
– Distributed sensors operating across multiple geographic locations and phenomenologies (i.e. optical, RADAR, and passive Radio Frequency (RF));
– Standardization of sensor tasking and data interchange formats;
– Open-source and/or sharable software applications for astrodynamics processing, data association/correlation/fusion, and error estimation;
– Common performance metrics and display formats to ensure consistency of operations and validity of assessments;
– Space Domain Awareness (SDA) areas:
  – Space object tracking and orbit characterization, collision and avoidance warning;
  – Space weather and environmental monitoring/reporting;
  – Space radio frequency interference characterizations and attribution against satellite control links and communication services.

EXPERIMENT OBJECTIVES
– Demonstrate and evaluate relevant data exchange/storage standards and decision support concepts; – Evaluate sufficiency of existing standards to describe space objects, events, and models, to support decision-making and space command and control; – Develop and demonstrate methods to fuse hard (physics-based) and soft (human-based) information; – Exercise existing methods and models to forecast space environment conditions that have quantifiable effects and impacts on space services and capabilities; – Exercise existing methods and models to forecast space environment conditions that influence space object events, such as collisions, re-entries, and breakups; – Exercise improved methods and models for quantifying, assessing, predicting, and mitigating Radio Frequency Interference (RFI); – Exercise existing data association methods for new space object discovery, space object identification, and track custody maintenance; – Experiment with improved processes to more accurately characterize sensor level errors and to improve space object detection, tracking, identification, and characterization; – Demonstrate and evaluate new processes that enable and support an SSA Common Operating Picture to improve decision-making and space command and control; – Demonstrate and evaluate techniques to automate routine Space Domain Awareness-related processing and data exchange; – Demonstrate and evaluate approaches to integrate and share knowledge of the current operational status of the NATO space systems, including knowledge of space environment effects and impacts.

Table 3: Scope and objectives of NATO's "Collaborative Space Domain Awareness Data Collection and Fusion Experiment".[47]

Inclusion of Space in the Category of Hybrid Threats

Hybrid threats are listed as one of seven categories[a] in the December 2016 Joint Declaration of the EU and NATO Councils which called for improved "mutual relations".[48] In the 2017 EC report on the implementation of the "Joint Framework on countering hybrid threats – a European Union response", the Commission also proposed to expand the monitoring of hybrid threats to space infrastructures.[49] In this connection, the Commission stated that: "within the context of the Space Strategy and European Defence Action Plan, the Commission will propose to increase the resilience of space infrastructure against hybrid threats, in particular, through a possible extension of the Space Surveillance and Tracking scope to cover hybrid threats, the preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependent on time synchronization".[50]

In 2016, the EU Hybrid Fusion Cell was established within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS), to receive, analyze and share both classified and open source information from the EEAS, EC and EU Member States on indicators and warnings related to hybrid threats with the goal of informing the EU's strategic decision-making processes (including security risk assessments).

a The other six are operational cooperation, cyber security and defence, defence capabilities, defence industry and research, exercises, and defence and security capacity building.

Separately, the European Centre of Excellence for Countering Hybrid Threats was launched in October 2017 under the joint auspices of the EU and NATO to encourage strategic dialogue and conduct research and analysis on hybrid threats. The Center's work has largely been dedicated to producing white papers, conducting training courses, and providing workshops to policymakers and practitioners.[51]

	MISSION
EU Hybrid Fusion Cell	to gather information and intelligence from Member States to inform decision-makers both in EU institutions and individual Member States.
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)	to establish a research institution that can conduct sound analysis, organize training courses and exercises for EU Member States and NATO allies.

Table 4: Missions of EU Hybrid Fusion Cell and European Centre of Excellence for Countering Hybrid Threats

Interaction between the EU Fusion Cell and the NATO Hybrid CoE in Finland is seen as an important element of EU/NATO cooperation on hybrid threats. Sharing intelligence analyses and assessment work is designed to reduce uncertainty and enhance situational awareness. Another important aspect is improving coordination via joint exercises, also called upon in the 2016 Joint Declaration.[a] The "Parallel and Coordinated Exercises" (PACE) concept was endorsed by NATO's Council Operations and Exercises Committee (COEC) in December 2016 and was noted by the EU Political and Security Committee (PSC) in February 2016.[52] In 2017, the first PACE took place to practice preparedness in a hybrid scenario – EU CYBRID 2017, EU PACE17 and NATO's CMX17.[53]

Figure 8: European Union Ministers of Defense taking part in the simulated cyber attack exercise EU CYBRID 2017 in Tallinn, Estonia. (Credit: Annika Haas, EU2017EE)

The EU CYBRID 2017, organized by Estonia during its European Council Presidency in cooperation with the European Defence Agency (EDA), was the first high-level tabletop exercise with the participation of EU Defense Ministers focused on cyber threats. It sought to assess the status of coordination at a political level and potential knock-on effects of an offensive cyber campaign. Situational awareness, crisis response mechanisms and strategic communications were at the center of this exercise.[54] EU PACE17 was conducted in parallel to classified NATO CMX17.[55]

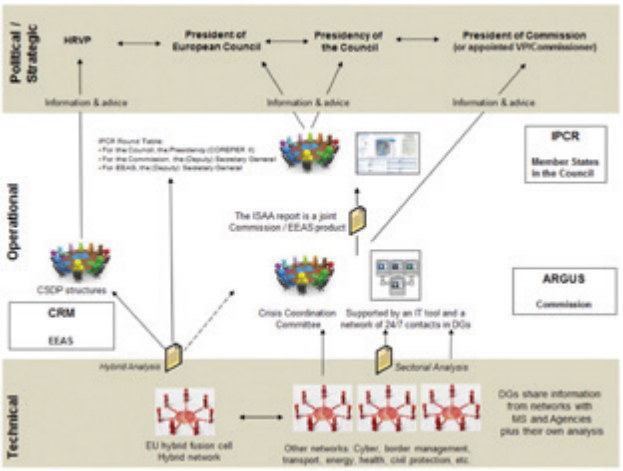


Figure 9: Information Flow in case of a hybrid threat (source: European Commission).[56]

Understanding space hybrid operations and their knock-on effects should be added to any national or Europe-wide pre-crisis planning. A somewhat expanded scope of space hybrid operations (by, for example, including the E&F elements), will assist in configuring proper management of a form of warfare deliberately wrapped in ambiguity and deception and designed to thwart effective allied responses largely via "incrementalism".

a The Declaration stipulates that EU and NATO should step up their "coordination on exercises, including on hybrid threats, by developing as the first step Parallel and Coordinated Exercises for 2017 and 2018". (EEAS (2017). *Second Progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016.* Available at: http://club.bruxelles2.eu/wp-content/uploads/2018/03/cooperationotan-ue-rap@ue171130.pdf, (EEAS (2017) 1507 REV 1).

Strengthened Deterrence via Space Partnerships

As hybrid threats are constantly evolving, adaptive countermeasures will have to be continuously developed. Collaboration – intra-European, transatlantic and international – represents a strategic pillar in managing these threats. It can help improve resiliency and deterrence via coordination of actions and preventive measures. Programmatic decisions need to be considered in an overall strategic framework that has a much bolder and forward-leaning European posture on space security. Current national strategies of European countries highlight a growing readiness and willingness of Member States to build out more robust European cooperation in space security. France declares, in this regard, that "a European approach to this topic of mutual interest will be promoted in various areas, including space surveillance".[57]

There are strong foundations to elevate the priority of this issue area in the transatlantic context, including through the Five Eyes and/or NATO. The United States fully recognizes the challenges related to operating in a "grey zone" environment. It observes, in its National Security Strategy (NSS) that "adversaries and competitors became adept at operating below the threshold of open military conflict and at the edges of international law" and that deterrence must be extended across all domains (including space) and "must address all possible strategic attacks".[58]

Similarly, The National Defense Strategy (NDS) specifically references China and Russia's "increased efforts short of armed conflict" and "deliberately blurring lines between civil and military goals".[59] If left unattended to, adversaries may become emboldened to intensify these activities raising the escalatory potential. In contrast to this blunt truth-telling, Europe still has a hard time bringing itself to "name names" of the two obvious state perpetrators of the current counterspace threats facing us (including their "go to" state-owned enterprises for the global space sector). Perhaps this level of caution is justified at this time (presumably for commercial and political reasons) but will need to evolve.

Although the current U.S. Administration follows an "America first" policy, President Trump conceded in January 2018 that even though his policies always aim to put America first, it "does not mean America alone." The benefits of alliances and partnerships contribute to the four lines of effort described in the implementation plan for the NSS (i.e. mission assurance; deterrence and warfighting; organizational support; and creating conducive domestic and international environments for U.S. space objectives).[60]

While there exists a clear transatlantic gap with regard to treating space security concerns, both sides fortunately recognize the bottom-line requirements for collaboration. Other partnerships can be added once the core (including Japan) is solidified. Indeed, opportunities abound for a wide array of new global partnerships, but the prospects for success will remain shaky so long as Europe is unwilling to openly identify China and Russia as the leading counterspace threats and confront their predations via a creative, non-kinetic strategy (e.g. one element of which is interrupting their "space sector capture" activities now in evidence worldwide).

Figure 10: U.S. Strategic Command (USSTRATCOM) leads Space Situational Awareness (SSA) Tabletop Exercise (TTX)/GLOBAL SENTINEL. The 2016 event provided an opportunity to develop and implement processes for partners from Australia, Canada, France, Germany, Japan, the United Kingdom, and commercial entities to collaborate on combined SSA operations. (Credit: USSTRATCOM)

IV. Recommendations

As evident from the "Key Findings", a number of activities dealing directly or indirectly with space hybrid operations are now underway in Europe. To accelerate this positive momentum, consideration should be given to the following recommendations:

- Elevate further the visibility of space hybrid operations so that this rapidly evolving threat is decisively taken off of "back-burner" status;

- Work to identify capability gaps, including the tracking and mapping of space incidents and the quick ability to differentiate between anomalies and space hybrid operations;

- Organize regular meetings of space security officials and experts to discuss the latest developments in this threat environment;

- Organize tabletop exercises and simulations to rehearse the operational aspects of detecting, attributing, characterizing and reacting to space hybrid incidents;

- Educate and train personnel in operations centers concerning these threats, including the E&F "space sector capture" predations of China and Russia globally;

- Review classification standards related to these threats to enable partner and allied access to essential information;

- Include these threats in the development of a Space Domain Awareness (SDA) architecture;

- Consider cross-domain deterrence or response options in the E&F space by putting at risk continued unfettered access to the international trading and financial systems by malevolent Chinese and Russian space-related, state-owned enterprises (several of which are publically-traded in Western capital markets).

Glossary of Acronyms

ADR	Active Debris Removal
ASAT	Anti-Satellite Weapon
ASI	Italian Space Agency
CDTI	Spanish Centre for the Development of Industrial Technology
CHEC	China Harbour Engineering Company
CLTC	China Satellite Launch & Tracking Control General
CNES	French Government Space Agency
COEC	Council Operations and Exercises Committee
CONAE	Nacional de Actividades Espaciales
DLR	German Aerospace Center
E&F	Economic and Financial Operations
EC	European Commission
EDA	European Defence Agency
EEAS	European External Action Service
EMP	Electromagnetic Pulse
ESA	European Space Agency
EU	European Union
EU INTCEN	EU Intelligence and Situation Centre
GaAs	Gallium Arsenide
GDP	Gross Domestic Product
GEO	Geosynchronous Orbit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HPM	High-Power Microwave
Hybrid CoE	European Centre For Excellence for Countering Hybrid Threats
InP	Indium Phosphide
ITU	International Telecommunication Union
ISR	Intelligence, Surveillance, and Reconnaissance
JSpOC	U.S. Joint Space Operations Center
LE	London Economics
LEO	Low Earth Orbit
LTA	NATO Long Term Aspect
MEO	Medium Earth Orbit
NATO	North Atlantic Treaty Organization
NDS	National Defence Strategy
NSS	National Security Strategy
PACE	Parallel and Coordinated Exercises
PLA	Chinese People's Liberation Army
PNT	Positioning, Navigation, Timing
PSC	EU Political and Security Committee
RADAR	Radio Detection and Ranging
RF	Radio Frequency
RFI	Radio Frequency Interference
RPO	Rendezvous and Proximity Operations
SatCen	EU Satellite Center
SATCOM	Satellite Communications
SDA	Space Domain Awareness
SOEs	State-Owned Enterprises
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking
STM	Space Traffic Management
STO	Science and Technology Organization
UK	United Kingdom
UKSA	United Kingdom Space Agency
UN	United Nations
U.S.	United States
UWB	Ultrawideband

Annex

Annex 1: Roundtable Program

Prague Security Studies Institute

Space Security Roundtable — May 18, 2018, 09:00 – 14:00

Responding to Unconventional Threats to Europe's Space Operations
AGENDA

Venue: Café Louvre
Národní 22
110 00 Prague 1
www.cafelouvre.cz/en/

Background: See Concept Paper

Proceedings:

08:30–9:00 Coffee and Registration

Welcoming Remarks and Introduction of Roundtable Objectives

09:00–09:20 Dr. Jana Robinson, PSSI Space Security Program Director

The roundtable consists of two sessions of approximately 95 minutes each. During each session, introductory remarks will set the scene for the discussions that are reflective of the key themes: policy and market effects stemming from space hybrid risks and threats; and Europe's readiness to manage these unconventional threats. The aim of this roundtable is to capture the concept of space hybrid threats (i.e. intentional, mostly reversible, and often harmful, space actions/activities conducted just below the threshold of requiring a meaningful military or political retaliatory response), assess the level of awareness and preparedness, as well as offer policy recommendations concerning resilience, effective deterrence and crisis management measures with regard to these threats.

The roundtable will be held under the Chatham House Rule (i.e. participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be directly revealed, including by inference).

↗ PSSI.CZ

Prague Security Studies Institute

Session One – Policy and Market Effects Stemming from Space Hybrid Threats

Currently, no mapping and effective deterrent structures exist addressing space hybrid risks and attacks (via established norms, active dissuasion, or accountability/enforcement measures). These threats are almost sure to grow as space serves as a force-multiplier for global power projection and influence on the part of state actors. There are likewise few discussions ongoing concerning how these risks and threats impact on broader security architectures. The goal of this session is to discuss the nature of space hybrid threats and the major security risks stemming from them.

09:20–09:40 Remarks by Dr. Kai-Uwe Schrogl (ESA), Editor, Handbook of Space Security, Springer International Publishing
"The Trajectory of Space Mission Assurance"

09:40–10:55 Discussion among participants

10:55–11:15 Coffee Break

Session Two – Europe's Readiness to Manage Risks and Threats to Space

The goal of this session is to assess Europe's readiness to respond cohesively and effectively to risks posed to spacecraft operating in space, as well as to threats and space hazards they may face. The establishment of foundational principles related to security, safety and sustainability of space operations can help build a political case for accelerated resilience and deterrence structures.

11:15–11:35 Remarks by Dr. Pascal Faucher, Chairman, EU SST Consortium
"Europe's Efforts in Safeguarding Space Infrastructure and Requirements for Resilient, Stable and Sustainable Space"

11:35–12:50 Discussion among participants

12:50–13:00 Closing Remarks
Dr. Jana Robinson, PSSI Space Security Program Director

13:00–14:00 Buffet Luncheon

Annex 2: Participant List

Prague Security Studies Institute

Space Security Roundtable

Responding to Unconventional Threats to Europe's Space Operations

May 18, 2018, Venue: Café Louvre, Národní 22, 110 00 Prague 1

LIST OF PARTICIPANTS

Stylianos Argyrakis
Embassy of Greece in Prague
Greece

Colin Armstrong
Head of Space Security Policy
United Kingdom Space Agency
United Kingdom

Marc Becker
Researcher
Hertie School of Governance
Germany

Petr Boháček
Associate Fellow
Association for International Affairs (AMO)
Czech Republic

Jakub Brož
Deputy Head of International Defence-Industrial Cooperation Unit
Ministry of Defence of the Czech Republic
Czech Republic

Lapo Degl'Innocenti
Project Assistant
Prague Security Studies Institute
Czech Republic

Giovanni Dionisi
Embassy of Italy in Czech Republic
Italy

Antal Disztl
Counsellor
Embassy of Hungary in Prague
Hungary

Pavel Ditmar
Logistics Manager
Prague Security Studies Institute
Czech Republic

Bohumil Doboš
Institute of Political Studies
Faculty of Social Sciences, Charles University
Czech Republic

Pascal Faucher
Chairman
EU SST Consortium
CNES HQ – French Space Agency
France

Amelie Gravier
Project Manager – Secretary of EU SST Consortium
CNES HQ – French Space Agency
France

Tomáš Kopečný
Director of Defense Industrial Cooperation Department
Ministry of Defence of the Czech Republic
Czech Republic

Václav Kobera
Director, Intelligent Transport Systems, Space Activities and R&D Department
Ministry of Transport
Czech Republic

Petr Lang
Program Director
Prague Security Studies Institute
Czech Republic

↗ PSSI.CZ

Attila Matas
Regulatory Consultant
OrbitSpectrum

Giulia Pavesi
Project Assistant
Prague Security Studies Institute
Czech Republic

Regina Peldszus
Policy Officer
Department of Space Situational Awareness
German Aerospace Center (DLR) Space Administration
Germany

Lisa Perrichon
Research Intern
European Space Policy Institute
Austria

Jana Robinson
Space Security Program Director
Prague Security Studies Institute
Czech Republic

Michael Romancov
Political Geographer, Institute of Political Studies, Faculty of Social Sciences
Charles University
Czech Republic

Johanna Salovaara-Dean
Embassy of Finland in Prague
Finland

Juan José Sanz Aparicio
Deputy Head of Mission
Embassy of Spain in the Czech Republic
Spain

Kai-Uwe Schrogl
Chief Strategy Officer
European Space Agency (ESA)
France

Martina Šmuclerová
Senior Fellow
Prague Security Studies Institute
Czech Republic

Ladislav Stahl
Ministry of Defence
Czech Republic

Adam Strauch
Masaryk University
Czech Republic

Jean-Jacques Tortora
Executive Director
European Space Policy Institute
Austria

Alyssa Wilson
Assistant Researcher
Prague Security Studies Institute
Czech Republic

↗ PSSI.CZ

Annex 3: International Legal Perspective on Space Hybrid Operations

From the perspective of international law it is essential to have a clear definition of "space hybrid operations" in order to delimit the possible reactive measures.

If the space hybrid operation amounts to an armed attack in light of Article 51 of the UN Charter, a reactive measure in the form of the right to self-defence is lawful. In other words, defensive recourse to the use of force and the right of the target to strike back is legally permissive. It raises the question, however, of how to define an armed attack in the specific physical conditions of Outer Space? Which iteration of space hybrid interferences might constitute an armed attack?

Beyond conventional military attacks, other space service disruptions might be judged, most practically, similarly to cyber attacks, via the "effects-based doctrine". It means that we assess the qualification of the attack in light of the consequences and damages caused. If a particular space hybrid disruption causes substantial harm and damages, the quantity and quality of which is equivalent to the destruction produced by a regular conventional armed attack (e.g. deactivation of data/signals paralyzing the functioning of the critical infrastructure of the state causing significant damage or even fatalities), the qualification as "armed attack" might apply.[a]

If a space hybrid operation does not attain the level of an armed attack but is qualified as illegal, there exists the right to apply countermeasures or reprisals. Countermeasure/reprisal is an act which is in itself illegal, but has been made acceptable in retaliation for the commission of an earlier illegal act by a state actor. Examples of countermeasures are traditional economic, financial or political sanctions. It is therefore essential to determine which of the hybrid disruptions constitute an international wrongful act. We may identify applicable rules banning such activities or initiate a new set of rules.

If the space hybrid operation is qualified as lawful, reactive measure can reportedly only take the form of pressure or coercion called retorsion (i.e., an unfriendly and harmful act which is a lawful retaliation against an injurious activity of another state, the objective of which is to hurt the perpetrator's interests with the aim of modifying its conduct). If the space hybrid operation is viewed as harmful interference under Art. IX of OST, it is important to note that this provision does not qualify the harmful interference as such as being illegal. Art. IX of OST only lays down the legal obligation for states to resort to consultations with respect to possible harmful interference.

a For the official guidance on the definition of an "aggression"/"armed attack" see GA RES 3314 (XXIX), Art. 3 - note esp. the attribution of acts of paramilitary, mercenaries, non-governmental entities etc.

About PSSI

The Prague Security Studies Institute

The Prague Security Studies Institute (PSSI) is a non-profit, non-governmental organization established in early 2002 to advance the building of just, secure, democratic, free market societies in the Czech Republic and other post-communist states. PSSI's mission is to build an ever-growing number of informed and security-minded policy practitioners dedicated to the development of democratic values and institutions, as well as protecting them from various traditional and asymmetric, hybrid threats. PSSI offers programs that help meet the critical requirements associated with equipping new generations of young leaders to manage the complex, security-related challenges of the 21st century.

To fulfill its mission, PSSI conducts a broad range of activities under its Security Scholars Program, Space Security Program, Economic & Financial Threat Program and Transnational Security Program. PSSI aims to identify and analyze geopolitical flashpoints and emerging threats regionally and globally and to propose sound and achievable policy options to deter and defeat hybrid warfare strategies and other forms of external aggression as well as security-relevant internal governance abuses. PSSI has a transatlantic footprint with its partner organization PSSI Washington. **pssi.cz**

PSSI Space Security Program

PSSI has been at the forefront of the European space security debate, producing analyses and international conferences for the international space community. The Institute, in partnership with PSSI Washington, initiated in 2011 what is now regarded as the leading NGO conference series in this field. Four such international conferences have been convened to date, involving leading space security experts and senior officials from Europe, the Unites States and Japan. Two were held in Prague, one in Tokyo, and one in Washington, DC. The key partnering organizations included ESA's European Space Policy Institute, the Japanese Prime Minister's Office of National Space Policy, the Secure World Foundation, and the Center for Strategic and International Studies. PSSI is planning to hold the next event in June 2019.

In 2015, PSSI helped configure and structure an academic course entitled, "Space Security in the 21st Century", taught within the curriculum of Charles University's Master's Degree Program in International Security Studies. Other educational venues in this field include PSSI's Security Scholars Program and its NATO Summer School. In the academic year 2018–2019, it will likewise begin to fund an approved Ph.D. scholarship in Space Security at Charles University in Prague.

Presently, PSSI is seeking to develop the most effective means to counter what it terms "space hybrid operations". It is likewise offering a creative toolkit for allied pre-crisis planning and management via promoting the institutionalization of behavioral norms, strengthened resiliency, and effective deterrence and accountability/enforcement measures. The latter involves economic and financial (E&F) cross-domain responses to space-related disruptions and/or attacks.

Finally, besides its widely recognized conference series, PSSI actively contributes to the transatlantic space security debate through roundtables, publications, speaking engagements, and analyses.

Acknowledgements

The authors of this report would like to express their gratitude to the roundtable participants for sharing their time, expertise, insights and observations. The roundtable benefited greatly from their interventions, including the keynote session introductions, delivered by Dr. Pascal Faucher, Chairman of the European Union Space Surveillance and Tracking (EU SST) Consortium and Dr. Kai-Uwe Schrogl, Chief Strategy Officer at the European Space Agency (ESA) and Chief editor of Springer Publishing House's Handbook of Space Security.

Sincere appreciation is also extended to the roundtable team which worked diligently to assist in organizing this event: Petr Lang, PSSI Program Director and Pavel Ditmar, PSSI Logistics Manager. Finally, we want to thank the following individuals for their expert assistance: PSSI Senior Fellow Martina Šmuclerová, and PSSI's Project Assistants Lapo Degl'Innocenti, Lisa Perrichon, and Jakub Pražák.

About the Authors

Jana Robinson

Dr. Jana Robinson is currently Space Security Program Director at the Prague Security Studies Institute (PSSI). She previously served as a Space Policy Officer at the European External Action Service (EEAS) in Brussels, as well as a Space Security Advisor to the Foreign Ministry of the Czech Republic. From 2009 to 2013, Ms. Robinson worked as Resident Fellow at the European Space Policy Institute (ESPI), seconded from the European Space Agency (ESA), leading the Institute's Space Security Research Programme.

Prior to joining ESPI, Dr. Robinson served as Development Director at PSSI from 2005 to 2009, and administered its affiliate organization in Washington DC, PSSI Washington. Dr. Robinson is an elected member of the International Institute of Space Law (IISL) and the International Academy of Astronautics (IAA). She is also a member of the Advisory Board of the George C. Marshall Missile Defense Project of the Center for Strategic and International Studies (CSIS) in Washington, D.C.

Ms. Robinson holds a Ph.D. from the Charles University's Faculty of Social Sciences, Institute of Political Studies, in the field of space security. She also holds two Master's Degrees, from George Washington University's Elliott School of International Affairs and Palacky University in Olomouc, respectively. She received scholarships to attend the International Space University's (ISU) 2009 Space Studies Program (SSP09), the 2008 Summer Training Course at the National Taiwan Normal University in Taipei, and a one-year course of study at Shanghai University 1999-2000.

Martina Šmuclerová

Dr. Martina Šmuclerová is a Senior Fellow at PSSI. As an international legal expert and university lecturer, she provides counsel in Public International Law, with an emphasis on Space Law and Law of International Security.

Dr. Šmuclerová previously served at the Czech Ministry of Foreign Affairs as a diplomat and international lawyer and represented the Czech Republic at the United Nations Committee for Peaceful Uses of Outer Space, the European Space Agency, the European Union and other fora. She initiated and led important international law projects such as the UN Space Debris Compendium.

Dr. Šmuclerová is a Senior Lecturer at Institut d'études politiques de Paris (SciencesPO) and teaches various courses in Public International Law, including Space law in collaboration with ESA. She received her Ph.D. in Public International Law (2010) and DEA/M.A. in International Law and International Organizations

(2003) from the Law School of Sorbonne University in Paris (Universite Paris 1 Pantheon-Sorbonne). She holds a French Government Scholarship and other awards. Dr. Šmuclerová is a member of the European Society of International Law and Société française pour le droit international.

Lapo Degl'Innocenti

Lapo Degl'Innocenti worked for PSSI as a Project Assistant from November 2017 – June 2018. He is enrolled in the Master's Degree Program in European and International Studies at University of Trento, Italy. He has been admitted to a double degree programme and is currently taking courses at the Metropolitan University in Prague.

He holds a Bachelor's Degree from the Department of Economic Development and International Cooperation at the University of Florence, Italy, with his thesis on International Space Law and Outer Space Exploitation. He focused his studies on international security threats related to the concept of global commons. Mr. Degl'Innocenti likewise attended courses on policy writing taught by the Enlargement Directorate Policy Officer of the European Commission.

Lisa Perrichon

Lisa Perrichon is a Project Assistant at the Prague Security Studies Institute (PSSI). She also works as a Research Associate at the European Space Policy Institute (ESPI). She previously worked as a Lecturer at the Silpakorn University International College (SUIC) in Thailand between 2014 and 2016. Prior to joining the Thai Ministry of Education, she worked as a Project Manager for the French Ministry of Foreign Affairs in Thailand and Iraq from 2011 to 2014.

Ms. Perrichon holds two Master's Degree from the University of Glasgow and the Charles University's Faculty of Social Sciences, Institute of Political Studies, in the field of International Security and Strategy. She was awarded a Certificate of Intelligence Analyst from the Ostbayerische Technische Hochschule Regensburg (OTR) in 2016. Ms. Perrichon also holds a Master's Degree in Intercultural Management and Negotiation from the University of Bordeaux and a Bachelor of Business from the University of Limoges. She received scholarships to attend the Friedrich-Alexander University Erlangen-Nürnberg in 2008 and the Dundalk Institute of Technology in 2009.

Jakub Pražák

Jakub Pražák is a Project Assistant at the Prague Security Studies Institute (PSSI). He is enrolled in two Master's Degree programs at the Charles University in Prague – Security Studies and International Relations. He holds a Bachelor's Degree in Political Science and International Relations at the Charles University's Faculty of Social Sciences. He also spent a semester abroad at the Tallinn University in Estonia. His areas of interest are astropolitics and space security. His bachelor thesis focused on ASAT Weapons and his current research involves utilization of Active Debris Removal Systems as an Anti-Satellite Weapons. He was an intern at the Czech Ministry of Defence and at the Czech National Cyber and Information Security Agency. He is also involved in student activities via Political Science Club organizing public lectures and debates.

Bibliography

1 Freedberg, S., (2018). 'Russia's Real Target Is US Alliances & Ukraine, Not Elections: CIA Veterans', *Breaking Defense*. Available at: https://breakingdefense.com/2018/06/russias-real-target-is-us-alliances-ukraine-not-elections-cia-veterans/, (June 11, 2018).

2 Freedberg, S., (2018). 'Russia, China Are Outmaneuvering US: Generals Recommend New Authorities Doctrine', *Breaking Defense*. Available at: https://breakingdefense.com/2018/06/russia-china-are-outmaneuvering-us-generals-recommend-new-authorities-doctrine/?utm_campaign=Breaking%20Defense%20Land&utm_source=hs_email&utm_medium=email&utm_content=63905514&_hsenc=p2ANqtz-9lV9BFszMA_XBT95-6_wl8P9G-YI7VbTBpNefGXmXJBtV28UqlYoZb7SIWjpQ4GovM_bdpJOd4vkfuaPYIlYDNuVksGg&_hsmi=63905514, (June 15, 2018).

3 Tran, P. (2018). 'Foreign governments are approaching French satellites in orbit, says space commander', *Defense News*. Available at: https://www.defensenews.com/space/2018/01/26/foreign-governments-are-approaching-french-satellites-in-orbit-says-space-commander/, (January 26, 2018).

4 Vedda, J. & Hays, P. (2017). 'Major Policy Issues in Evolving Global Space Operations,' *Mitchell Institute*, (Policy Paper Vol.9, p.2), Available at: http://www.airforcemag.com/DRArchive/Documents/2017/120517_MitchellPolicyPapers_SpaceOperations.pdf, (December 2017).

5 Stein, J. (1988). 'Satellites, anti-satellite weapons and security', *The RUSI Journal*, 133(4), pp.49-51.

6 Sorge, M. and Peterson, G. (2015). *How to Clean Space: Disposal and Active Debris Removal*. [online] Web.archive.org. Available at: https://web.archive.org/web/20180303033217/https://aerospace.org/crosslinkmag/fall-2015/how-to-clean-space-disposal-and-active-debris-removal/, [Accessed 29 Jun. 2018].

7 Hitchens, T. (2014). *Debris Removal/Rendezvous and Proximity Operations: Looking at Policy Implications*. [ebook], Available at: http://www.unidir.ch/files/conferences/pdfs/debris-removal-rendezvous-and-proximity-operations-looking-at-policy-implications-en-1-970.pdf, [Accessed 29 Jun. 2018].

8 Robinson, J. (2018). 'Cross-Domain Responses to Space Hybrid Provocations via Economic and Financial Statecraft', *USSTRATCOM 2018 Deterrence and Assurance Academic Alliance Conference*. Available at: pssi.cz/download/docs/552_paper-2018-deterrence-and-assurance-conf-final.pdf, (March 16, 2018).

9 Information in this table was adopted from various sources, including: Harrison, Johnson, Roberts, (2018). *Space Threat Assessment 2018*. (Aerospace Security, 11 April 2018), Available at: https://aerospace.csis.org/space-threat-assessment-2018/?utm_source=CSIS+All&utm_campaign=6e7d894e9a-EMAIL_CAMPAIGN_2017_12_31&utm_medium=email&utm_term=0_f326fc46b6-6e7d894e9a-191654645; Weeden, Samson, (2018). *Global Counterspace Capabilities: an open source assessment*, (Secure World Foundation, April 2018). Available at: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf; Jafri, A. & Stevenson, J. (2018). *NSI Concept Paper, Space Deterrence: The Vulnerability-Credibility Tradeoff in Space Domain Deterrence Stability, (*Arlington, VA: Strategic Multi-layer Assessment (SMA)). Available at: http://nsiteam.com/sma-publications; Wilson, Tom, (2000). *Threats to United States Capabilities*, (Paper prepared for Prepared for the Commission to Assess United States National Security Space Management and Organization). Available at: https://fas.org/spp/eprint/article05.html#9.

10 Rosenfeld, E. (2014). 'Chinese hack US weather systems, satellite network: Wash Post', *CNBC*. Available at: https://www.cnbc.com/2014/11/12/chinese-hack-us-weather-systems-satellite-network-washington-post.html, (12 Nov 2014).

11 Robinson, J. (2018). 'Cross-Domain Responses to Space Hybrid Provocations via Economic and Financial Statecraft', *USSTRATCOM 2018 Deterrence and Assurance Academic Alliance Conference* (March 16, 2018). Available at: pssi.cz/download/docs/552_paper-2018-deterrence-and-assurance-conf-final.pdf

12 Assemblée Nationale (2016). *Audition du général Jean-Daniel Testé, commandant interarmées de l'espace*, Available at: http://www.assemblee-nationale.fr/14/cr-cdef/15-16/c1516048.asp, (Compte rendu n° 48, May 17, 2016).

13 Nakashima, E. (2015). 'Russian hacker group exploits satellites to steal data, hide tracks', *The Washington Post*, (September 9, 2015).

14 Tanase, S. (2015). 'Satellite Turla: APT Command and Control in the Sky', *Kaspersky Lab*, (Sept. 9, 2015).

15 Robinson, J. (2018). 'Cross-Domain Responses to Space Hybrid Provocations via Economic and Financial Statecraft', *USSTRATCOM 2018 Deterrence and Assurance Academic Alliance Conference*.

16 Geospatial World (2017). 'Russia's RSC Energia to develop remote sensing satellite for Egypt'. Available at: https://www.geospatialworld.net/news/russias-rsc-energia-develop-remote-sensing-satellite-egypt/, (January 13, 2017).

17 SpaceWatch ME (2017). 'Ethiopia Start Work Space Launch Vehicle Domestically Made Satellites', *SpaceWatch Middle East*. Available at: https://spacewatchme.com/2017/01/ethiopia-start-work-space-launch-vehicle-domestically-made-satellites/, (January 2017).

18 allAfrica (2018). 'Ethiopia, Russia Enter New Frontier', *allAfrica*. Available at: https://allafrica.com/stories/201804100937.html, (April 5, 2018).

19 Milne, S., MacAskill, E. (2015). 'South Africa spied on own government to get facts on joint project with Russia', The Guardian. Available at: https://www.theguardian.com/world/2015/feb/25/south-africa-spied-government-facts-joint-russian-project, (February 5, 2015).

20 Cody, E. (2007). 'China Builds And Launches A Satellite For Nigeria', *Washington Post*. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/13/AR2007051301264.html??noredirect=on, (May 14, 2007); Clark, S. (2011). 'Chinese Rocket Launches Powerful Nigerian Satellite Into Orbit', *Space.com*. Available at: https://www.space.com/13975-china-rocket-launching-huge-nigeria-satellite.html, (December 19, 2011); and Monks K. (2016). 'Nigeria plans to send Astronaut to space by 2030', *CNN*. Available at: https://edition.cnn.com/2016/04/06/africa/nigeria-nasrda-space-astronaut/index.html, (April 6, 2016).

21 Robinson, J. (2018). 'Cross-Domain Responses to Space Hybrid Provocations via Economic and Financial Statecraft', *USSTRATCOM 2018 Deterrence and Assurance Academic Alliance Conference* (March 16, 2018). Available at: pssi.cz/download/docs/552_paper-2018-deterrence-and-assurance-conf-final.pdf.

22 Office of the Assistant Secretary of Defense for Homeland Defense & Global Security (2015). *Space Domain Mission Assurance: A Resilience Taxonomy*, (September 2015).

23 Robinson J. & Bettman M. (2016). *Advancing the Trilateral Europe-U.S.-Japan Space Security Partnership - Conference Report*. Available at: http://www.pssi.cz/download/docs/379_conference-report.pdf, (p.10).

24 Ibid.

25 Ibid.

26 PwC (2016). *Study to examine the socioeconomic impact of Copernicus in the EU. Report on The socio-economic impact of the Copernicus programme*. Available at: http://www.copernicus.eu/sites/default/files/library/Copernicus_SocioEconomic_Impact_October_2016.pdf, (Brussels: European Commission, October 2016).

27 European Commission (2018). *Establishing the space programme of the Union and the European Union Agency for the Space Programme*. Available at: https://ec.europa.eu/info/law/better-regulation/initiative/245587/attachment/090166e5bb4d0, (SWD(2018) 327 final, Brussels, June 6, 2018).

28 European Commission (2016). *Copernicus: Market report.* Available at: http://www.copernicus.eu/sites/default/files/library/Copernicus_Market_Report_11_2016.pdf, (Luxembourg: Publications Office of the European Union. November 2016).

29 London Economics (2017). *The economic impact on the UK of a disruption to GNSS*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf.

30 Paxamericanafilm (2010). *CLIP- A Day Without Space*. [video] Available at: https://www.youtube.com/watch?reload=9&v=lLRdNEQqxAg [Accessed 13 Jul. 2018]; Benedict, R (2015). *If there were a day without satellites...* (2015). [video] Available at: https://www.youtube.com/watch?v=5sgM7YC8Zv4 [Accessed 13 Jul. 2018]; Hollingham, R. (2013). What would happen if all satellites stopped working? [online] BBC.com. Available at: http://www.bbc.com/future/story/20130609-the-day-without-satellites [Accessed 13 Jul. 2018].

31 NATO (2018). 'Point 19', *Brussels Summit Declaration*. Available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (July 11, 2018); and Lt CDR Kroeger, R. *et al.* (2017). 'Introducing Space Support to Operations', *The Three Swords Magazine.* Available at: http://www.jwc.nato.int/images/stories/_news_items_/2017/SPACE.pdf, (n.31, 2017).

32 International Telecommunication Union (2002). *Technical and operational characteristics of satellites operating in the range 20-375 THz*. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1590-0-200209-I!!PDF-E.pdf.

33 Robinson J. & Bettman M. (2016). *Advancing the Trilateral Europe-U.S.-Japan Space Security Partnership - Conference Report, p.5.* Available at: http://www.pssi.cz/download/docs/379_conference-report.pdf.

34 EUSST, (2018). *EU SST Governance*. [online] Available at: https://www.eusst.eu/project/who-we-are/.

35 EUSST, (2017). *EU SST Consortium governance, initial operation and current status*. Available at: https://www.b2match.eu/system/spaceweek2017-italy/files/6._Portelli.pdf?1511872177, (November 21th 2017, ASI, Roma), European Council (2018). *Report on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-2017)*. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF, (Brussels, May 3, 2018).

36 Source: European Commission (2018). Proposal - establishing the space programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU Available at: https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-space-programme-impact-assessment1_en.pdf, (Brussels, June 6, 2018).

37 European Commission (2014). *Decision No 541/2014/Eu Of The European Parliament And Of The Council*. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF.

38 European Commission (2018). *Report from the Commission to the European Parliament and the Council on the implementation of the Space Surveillance and Tracking (SST) support framework (2014-2017)*. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:fbafc703-4eb8-11e8-be1d-01aa75ed71a1.0021.02/DOC_1&format=PDF, (May 3, 2018).

39 European Commission (2018). 'Establishing the space programme of the Union and the European Union Agency for the Space Programme.'Available at: https://ec.europa.eu/info/law/better-regulation/initiative/245587/attachment/090166e5bb4d0, (SWD(2018) 327 final, Brussels, 6.6.2018).

40 Lieutenant Colonel Neumann, S. (2015). 'How Hollywood's Movie 'Gravity' Highlights NATO's Need for Space Situational Awareness', *JAPCC Journal Issue 20*. Available at: https://www.japcc.org/space-hollywoods-movie-gravity-highlights-natos-need-space-situational-awareness/.

41 NCIA, (2014). 'Space Support to Operations: NATO Dependencies on Space', TR/2014/SPW009481/01, (February 2014).

42 Fleischer, P. (2016). 'Above the Moon: NATO Space Policy', *Atlantic Council Future NATO*. Available at: http://futurenato.org/articles/above-the-moon-nato-space-policy/, (September 9, 2016).

43 STO NATO (2011). *Space Environment Support to NATO Space Situational Awareness*. Available at: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16297.

44 Lieutenant Colonel Console, A. (2017). 'Multinational Space Surveillance and Tracking Initiatives from a NATO Perspective', *JAPCC Journal Issue 23*. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Journal_Ed-23.pdf, (p.45-50).

45 STO NATO (2018). *Collaborative Space Domain Awareness Data Collection and Fusion Experiment*. Available at: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16519.

46 Ibid.

47 STO NATO (2018). *Collaborative Space Domain Awareness Data Collection and Fusion Experiment*. Available at: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16519.

48 NATO-EC (2017). *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Available at: https://www.nato.int/cps/ic/natohq/official_texts_133163.htm, (05 Dec. 2017).

49 European Commission (2017). *Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead*. Available at: http://europa.eu/rapid/press-release_IP-17-2064_en.htm.

50 European Commission (2017). *Implementation of the Joint Framework on countering hybrid threats - a European Union response*, (19.7.2017 JOIN(2017) 30 final).

51 Standish R., (2018). 'Inside a European Center to Combat Russia's Hybrid Warfare', *Foreign Policy*. Available at: https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/, (January 18, 2018).

52 Ibid., p.4.

53 Council of the European Union (2017). *Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17*. Available at: http://www.statewatch.org/news/2017/jul/eu-council-pace-crisis-management-exercise-plan-11256-17.pdf, (Brussels, 14 July 2017).

54 European Defense Agency, (2017). *First cyber exercise at EU ministerial level focuses on strategic decision-making*. Available at: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making, (September 7, 2017).

55 EEAS (2107). EU launches exercise to test crisis management mechanisms in response to cyber and hybrid threats, EU Press Release. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/32969/eu-launches-exercise-test-crisis-management-mechanisms-response-cyber-and-hybrid-threats_en, (September 28, 2017).

56 European Commission (2017). *Joint Staff Working Document – EU operational protocol for countering hybrid threats, "EU Playbook".* (Brussel, JOIN/2017/030 final).

57 European Council (2017). *Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17*. Available at: http://www.statewatch.org/news/2017/jul/eu-council-pace-crisis-management-exercise-plan-11256-17.pdf, (Brussels, July 14, 2017).

58 The White House (2017). *National Security Strategy of the United States of America*. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, (Washington, DC, December 2017: 27).

59 Department of Defense (2018). Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge. Available at: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, (Washington, DC: Department of Defense (January 2018): 2).

60 Assistant Secretary of Defense Kenneth Rapuano in his testimony to the House Armed Services Subcommittee on Strategic Forces, (March 2018).

Prague Security
Studies Institute