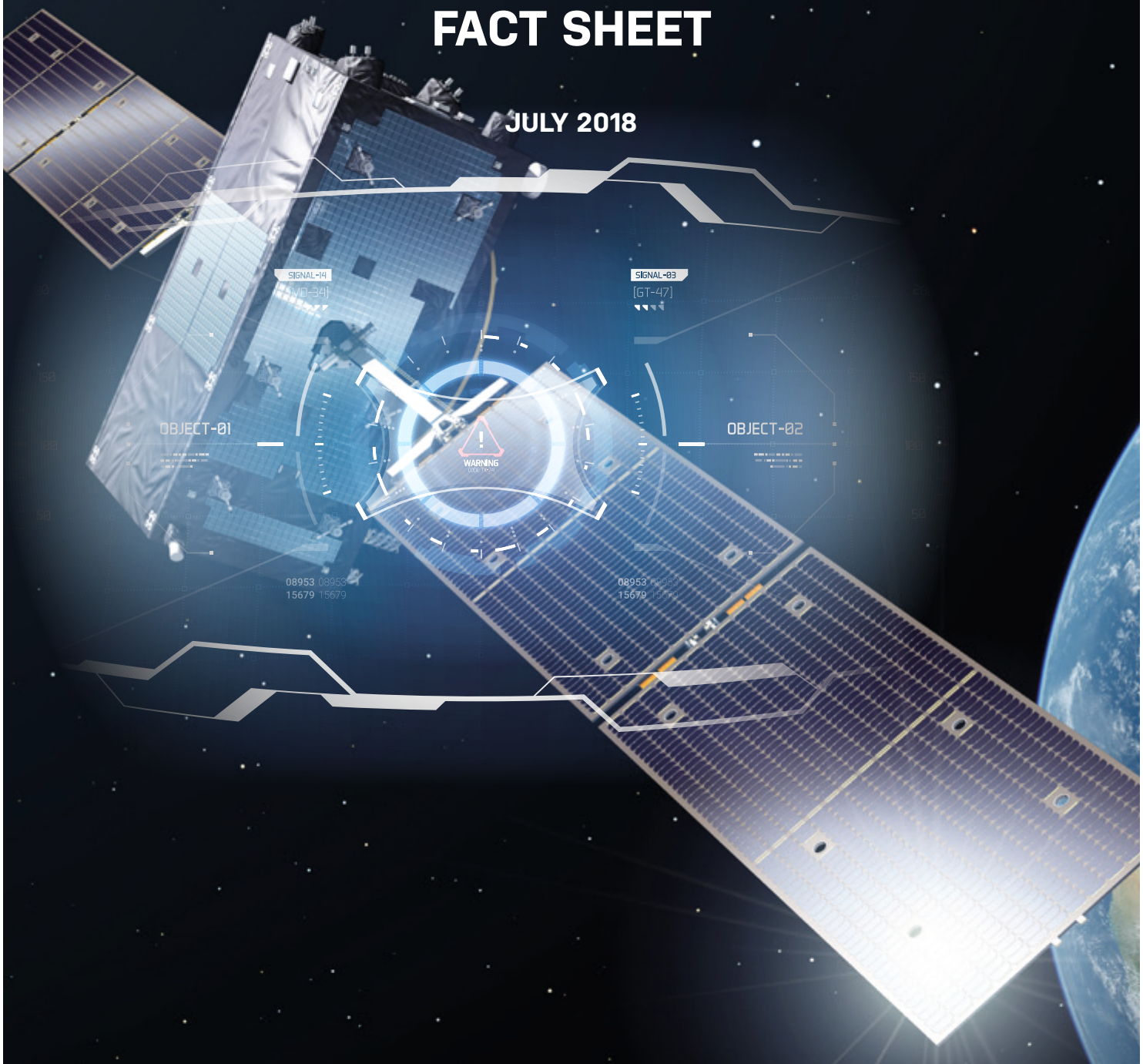
SPACE HYBRID OPERATIONS

FACT SHEET

JULY 2018



Prague Security Studies Institute

Space assets are of vital importance to the civil societies and militaries of an increasing number of countries. The global counterspace dynamic today is primarily driven by the U.S. – China – Russia rivalries, accompanied by other factors, such as a surge of new actors (including commercial operators) and proliferation of advanced space technologies. The combination of reliance on space for military operations and immensely important socio-economic services to most nations, and an increasing challenge to maintain space stability to help 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.

The spectrum of counterspace actions and threats are, at long last, of great concern worldwide due to their potential asymmetric, 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, rendezvous and proximity operations (RPO), 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"). 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[i]

Past examples include: China blinding a U.S. surveillance satellite in 2006; China hacking the U.S. weather satellite system in 2014; Russian military satellite engaging in close manoeuvers in the vicinity of two Intelsat satellites in geostationary orbit in 2015; Russia conducting close approaches to other space objects between 2015–2017; and Russia and China engaging in E&F "space sector capture" activities in countries like Argentina, Bolivia, Egypt, Belarus, Nigeria, Pakistan and South Africa.

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").

i 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.

Figure 1: Space assets are vulnerable to an attacks. An artist image of a laser weapon. Credit: Getty Images

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.

Due to the asymmetric effects for many, if not 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 by an adversary/competitor should best be thought of as a number of events, rather than a single incident, designed to probe the gaps in preparedness, readiness, allied coordination and response options. Better understanding these capability gaps permits an adversary to configure an effective strategy to gain a decisive advantage.

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

Increasingly, military and civilian 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. Accordingly, there is an urgent need to configure appropriate pre-crisis planning (including resiliency, deterrence, and cross-domain response options), as well as how to operate in a contested, degraded and operationally-limited space environment.

Consideration should be given to the following:

- 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 rapid 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 which can put at risk continued unfettered access to the international trading and financial systems by malevolent Chinese and Russia space-related, state-owned enterprises (several of which are publically-traded in Western capital markets).

For more information see PSSI's report entitled "Europe's Preparedness to Respond to Space Hybrid Operations". Available at: www.pssi.cz/download/docs/590_europe-s-preparedness-to-respond-to-space-hybrid-operations.pdf