Paper for the 2018 Deterrence and Assurance Academic Alliance Conference
"Thinking Outside the Silo: Creative Problem-Solving in Deterrence and Assurance"

Cross-Domain Responses to Space Hybrid Provocations via Economic and Financial Statecraft

March 2018

By Dr. Jana Robinson, The Prague Security Studies Institute

Introduction

To date, discussions concerning unconventional (or hybrid) warfare practices have been largely confined to terrestrial and maritime conflicts (e.g. Russia's operations in Crimea and Eastern Ukraine, its cyber campaigns in the U.S. and Europe, China's island-building/militarization in the South China Sea, North Korean nuclear brinksmanship, Iranian proxy conflicts and direct engagements in the Middle East, Chinese and Russian economic "nation-capturing" activities etc.). Space has been, for the most part, excluded from national and international gatherings and exchanges on this security policy portfolio, despite the fact that some of the same actors, mindsets and techniques are presently in play in the space domain as well (i.e. engaging in provocations just below the threshold of requiring meaningful allied retaliatory responses). Authoritarian space competitors seem intent on testing the resiliency of allied satellites, ground infrastructure and links using cyber attacks, jamming/spoofing and blinding, orbital manoeuvers, proximity operations and high-altitude ASAT tests, to name a few.

Two countries – China and Russia – stand out in possessing these and other counterspace capabilities and the political will to test them against "live" allied targets. It is Beijing and Moscow that are most actively using the space domain as a means to project power and influence for the purpose of advancing, and consolidating, their countries' strategic objectives. Moreover, the Kremlin and the Zhongnanhai are more closely collaborating than ever before on how to undermine American space primacy. These hard facts make it more urgent to assess the level of allied readiness to face more seriously disruptive space contingencies in the relatively near-term.

Temporary and reversible harmful interference can be, in many cases, plausibly denied, making it an attractive option for malevolent space actors. Skilled space hybrid operations enable a state actor to probe, intimidate, degrade, and even destroy targeted U.S. and allied capabilities without clear-cut attribution. To create even greater ambiguity, the attacker could make use of civilian or commercial space assets. An on-orbit, seemingly benign spacecraft could be equipped with a variety of warfighting capabilities (including lasers, radio frequency emitters, etc.).

We are already witnessing the proliferation of hybrid threats to space. Both active operations (such as cyberattacks, jamming or spoofing, dazzling, etc.) and passive ones (e.g. hiding or moving assets etc.) are already underway. For example, in 2006, China exercised the capability to blind a U.S. surveillance satellite.[1] During the annexation of Crimea, Moscow jammed communications and spoofed GPS systems.[2] In 2015, a Russian military satellite made several close manoeuvers in a vicinity of two Intelsat satellites in geostationary orbit (reportedly one of the first publically noted incidents of a commercial operator being approached by a foreign military satellite)[3]. Last year, Russia reactivated its satellite, Kosmos 2504, launched in 2015, and conducted manoeuvers close to the remnant of a weather satellite shot down by China in 2007.[4] In December 2017, French Joint Space Commander, Gen. Jean-Pascal Breton, admitted that the country's satellites have been closely inspected by foreign governments.[5]

These activities, and more not recounted, indicate a troubling trend, particularly as these operations have the potential to negate or disrupt critical U.S. and allied space systems. Also of concern is the upward trajectory of international geopolitical tensions that could ultimately implicate space.

---

[1] Harris, Francis." Beijing secretly fires lasers to disable US satellites", TheTelegraph (Sep 26, 2006), http://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html
[2] Pomerleau, Mark. "Threat from Russian UAV Jamming Real, Officials Say". C4ISRNET (Dec 20, 2016), http://www.c4isrnet.com/articles/threat-from-russian-uav-jamming-real-officials-say
[3] Gruss, Mike. " Russian Satellite Maneuvers, Silence Worry Intelsat," The Space News (Oct 9, 2015), http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/
[4] Ashok, India. "Is Russia prepping for space war? 3 mystery satellites reactivated but no one knows what they can do", International Business Times (May 22, 2017), http://www.ibtimes.co.uk/russia-prepping-space-war-3- mystery-satellites-reactivated-no-one-knows-what-they-can-do-1622695
[5] Tran, Pierre. "Foreign governments are approaching French satellites in orbit, says space commanter". DefenseNews (Jan 26, 2018), https://www.defensenews.com/space/2018/01/26/foreign-governments-are-approaching-french-satellites-in-orbit-says-space-commander/

The new U.S. National Security Strategy (NSS) observes 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".[6] Similarly, The National Defense Strategy (NDS) references China and Russia's "increased efforts short of armed conflict" and "deliberately blurring lines between civil and military goals".[7]

Accordingly, now is the proper time for the U.S. and the allies to consider their deterrence options and policy responses to space hybrid operations, both at the national and multilateral levels. Decision-makers need to discuss how best to prepare for reacting to provocations or disruptive actions in a "grey-zone" environment with imperfect attribution.

Given the fragility of the space domain and the destructive, cascading effects that "tit for tat" retaliation could unleash, the tool kit of deterrence and response options to unconventional threats needs to be expanded via creative measures drawn from the economic and financial domain.

Policy Implications of Space Hybrid Warfare Practices

As a critical enabler for security and defense-related missions, space is a key element of a nation's overall power projection capabilities. Taken together, the civilian, commercial, defense and intelligence uses of space provide a vast, and often interconnected, matrix of essential services. Accordingly, state actors utilizing, and operating in, space are constantly evaluating how to strike a proper balance between collaboration and operational dominance/control of space. This undertaking is especially sensitive concerning potential adversaries such as China and Russia.

The power projection strategies of these countries, often communicated through their actions, multilateral initiatives and public diplomacy priorities, have the potential to undermine global

[6] "National Security Strategy of the Unites States of America," Washington, DC: The White House (December 2017): 27, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[7] "Summary of the 2018 National Defense Strategy of the Unites States of America: Sharpening the American Military's Competitive Edge," Washington, DC: Department of Defense (January 2018): 2, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

efforts to preserve the stability of the space environment and sustainability of outer space. This is largely because of non-transparency, the clear primacy of military space activities and the lack of accountability.

While efforts to implement transparency and confidence-building measures, behavioral codes, and guidelines for space sustainability (such as those approved recently and in 2016 at the UN Committee on the Peaceful Uses of Outer Space) should continue, these measures alone generally cannot garner adequate compliance to serve as a true deterrent. Accordingly, they need to be reinforced by sound and robust space crisis management.[8] This is a stated objective in the new NDS.

The recently released NSS describes the current geopolitical environment as one characterized by the realist school of international relations. Beijing and Moscow subscribe to a number of the views expressed in Everett Dolman's "Astropolitics"[9], notably that for a state to remain sovereign it must, at minimum, prevent another state from gaining control of strategic locations, pathways and chokepoints. Moreover, control must be extended from "Terra" (or Earth), to "Terran" (or Earth space), as it does not only help facilitate long-term control of space, but offers near-term advantage on the terrestrial battlefield.[10] Although these are not new revelations, China and Russia have become considerably more emboldened and adept at employing unconventional methods to gain greater control of Earth space.

In June 2015, Deputy Defense Secretary Robert Work asserted that Russia and China pose threats to vital U.S. space capabilities and other U.S. technological weapons superiority.[11] Almost decade-and-half earlier, the Commission to Assess U.S. National Security, Space Management and

---

[8] The main focus of space crisis management is on efforts to identify those situations that are prone to threats to space assets and related services with the goal of preserving a stable space environment (source: Jana Robinson, "Space Crisis Management: Europe's Response," *European Space Policy Institute* 44 (February 2013): 20, http://www.espi.or.at/images/stories/dokumente/studies/ESPI_Report_44.pdf)

[9] Astropolitics is defined by Dolman as "the study of the relationship between outer space terrain and technology and the development of political and military policy and strategy" (Everett C. Dolman. *Astropolitik: Classical Geopolitics in the Space Age* (London and Portland, OR: Frank Cass Publishers, 2002), 15.)

[10] Everett C. Dolman. *Astropolitik: Classical Geopolitics in the Space Age* (London and Portland, OR: Frank Cass Publishers, 2002), 69-70.

11 Bill Gertz, "Star Wars, the Cold War Edition: Pentagon Girds for the Space War with Russia, China," The Washington Times (June 25, 2015), http://www.washingtontimes.com/news/2015/jun/25/pentagon-preps-space- warfare-russia-china/

Organization, observed that "China's military is developing methods and strategies for defeating the U.S. military in a high-tech and space-based future war'."[12]

Beijing's 2007 kinetic intercept of its own satellite demonstrated that China does not wish to remain a second-tier space power. Ashley Tellis, an expert on Asian strategic issues, pointed out that China's growing ASAT capabilities are part of its larger strategy of being positioned to confront superior U.S. capabilities.[13] Dean Cheng, who specializes in China's military doctrine, suggests that its military space program promotes China's "zonghe guojia liliang", or "comprehensive national security" and can serve as a potent diplomatic tool. Kevin Pollpeter, an analyst of China's space program and information warfare, noted that there is presently a PLA game plan to seize the initiative right at the beginning of a conflict, which has implications for allied protection of military centers of gravity (i.e. C4ISR nodes).[14]

Russia is likewise flexing its space-related muscles and is a big believer in exploiting the asymmetric advantages abundant in the space domain, particularly given its economic and financial constraints and its terrestrial hybrid warfare successes. This is, in part, why the EU and NATO felt compelled to establish in October 2017 the European Centre of Excellence for Countering Hybrid Threats.

Although this is just a snap-shot of the many geopolitical and technical factors at play, the bottom line is that space has become an essential force-multiplied for China and Russia's bid for expanded global influence and control. The NSS makes clear that the safety and long-term prosperity of the American people is at risk due to existing vulnerabilities in space being exploited by these and

12 Donald H. Rumsfeld et al., "Report of the Commission to Assess United States National Security Space Management and Organization: Executive Summary" (Washington DC, January 11, 2001), xiv and 22-23, http://www.fas.org/spp/military/commission/executive_summary.pdf
13 Ashley J. Tellis, "China's Space Weapons," Carnegie Endowment for International Peace (July 23, 2007), http://carnegieendowment.org/2007/07/23/china-s-space-weapons
14 Presentation by Kevin Pollpeter at a "SMA Space Panel Discussion: China's Perspectives on Space Deterrence and Escalation" (Washington, DC, February 16, 2018).

possibly other state actors.[15] The NDS adds that this more belligerent Chinese and Russian competition is strategic and operates "across all dimensions of national power".[16]

The unusual nature of counterspace threats also warrants intensified and expanded dialogue with U.S. partners in Europe and Asia (notably Japan) about when and how to take action in this often "grey-zone", if warranted. Moreover, the private sector needs to be fully engaged with respect to real-time communications, resilience and appropriate deterrence as its stakes in space continue to grow rapidly.

Dedicated partnerships focusing on prevention and preparedness, accompanied by governmental support for international space governance and potential cross-domain allied responses, are the right mix for ensuring space security over the long-term. To get this done, however, space hybrid threats must be integrated into broader security architectures and military planning. The U.S. takes this approach, but a number of allied governments do not.

Cross-Domain Responses via Economic and Financial Statecraft/Tools

The current menu of readily useable responses to unconventional space threats and disruptive action by China and Russia is arguably insufficient. As already mentioned, reactions within the space domain carry a number of potentially severe downside risks. As the U.S. has long been sensitive to these limitations, it has made clear, including in its new NSS, that it would respond to hostile actions in space "at a time, place, manner, and domain" of its choosing[17], thereby creating constructive ambiguity as well as flexibility.

Cross-domain response options are designed to dissuade an adversary from seeking to deliver asymmetric effects via space or penalize such a state convincingly, should it miscalculate and

[15] "National Security Strategy of the Unites States of America," Washington, DC: The White House (December 2017): 8, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[16] "Summary of the 2018 National Defense Strategy of the Unites States of America: Sharpening the American Military's Competitive Edge," Washington, DC: Department of Defense (January 2018): 1, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[17] "National Security Strategy of the Unites States of America," Washington, DC: The White House (December 2017): 31, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

venture forth. In this context, economic and financial (E&F) tools are particularly attractive. It is likely that Beijing and Moscow are simply not adequately taking into account that hostile behavior in space could put at risk elements of their domestic political stability and viability in the global markets (i.e., accepted participation in the international trading and financial systems including China's Belt and Road Initiative). Accordingly, such a prospect would likely alter their calculus in a manner favorable to U.S. and allied space security interests.

These E&F additions to the policy response menu would be consistent with the NSS and NDS. One of priorities of the NSS is to strengthen the rules-based international order, including shaping and reforming international financial and trade institutions. It distinguishes between countries that respect free and fair market principles and state-led economies that often show little regard for these principles.[18] It also makes clear that these competitors are regularly pursuing strategic objectives (such as "nation-capture" and leveraging undue dependencies) under the guise of benign commercial transactions.

The proverbial coin of the realm in the global markets is information. Understanding in detail the global operations of Chinese and Russian space-related, state-owned or -controlled enterprises (SOEs), and their corporate networks of subsidiaries, would represent a good starting point. Tracking and mapping the international transactions of these state-led companies would also reveal what these governments are doing, as opposed to what they are saying, which are frequently at odds.

This kind of systematic scrutiny would reveal that these enterprises often operate in security-sensitive countries, with high-risks partners (e.g. Iran, North Korea, Syria, Venezuela, Pakistan etc.). The networks of subsidiaries of these enterprises help them blur their identities and confuse the "risk management" and compliance side of the markets. This, in turn, equips them to engage in state-sponsored, space-related business activities designed to bolster their offensive capabilities in space – a form of E&F unconventional warfare.

[18] Ibid.: 17

The irony is that many of these Chinese and Russian enterprises (some cloaked as "private sector" firms) are, at the same time, seeking to build positive corporate reputations and brands globally, making them vulnerable to being publically exposed as "bad actors". Such "naming and shaming" could, for example, make prospective Western partners recoil if the "risk profile" of these firms were to rise and become more visible. Put simply, risk-relevant information made available to the global markets could itself serve as a penalty for reckless or malevolent behavior in space.

It can be argued that such corporate abusers should not be permitted to enjoy the best of both worlds – working to undermine a stable space environment while prospering as legitimate business partners in the global markets (including receiving unfettered access to allied debt and equity markets for large-scale funding). E&F response options, individually tailored to various space contingencies, would almost surely enhance the overall deterrence posture of the alliance in space and expand the toolkit to respond proportionately and without damaging space assets or risking a retaliatory spiral there.

Beyond "naming and shaming", Chinese and Russian state-controlled corporate facilitators of space hybrid warfare could be made to face unilateral or multilateral sanctions, such as (on the unilateral side) impeding the ability of Chinese or Russian space-related enterprises to operate within the U.S. or to do business with American corporate entities and persons elsewhere. Non-space-related enterprises operating in the U.S could also be targeted. Forging multilateral sanctions directed toward: the launch services/capabilities of these countries (when the U.S. is no longer held somewhat hostage to such Russian services/capabilities); technical cooperation; joint projects; and the benefits associated with select global business engagements involving space, would likely prove effective. Denying access of offending space-related entities to the U.S. financial system and the use of the dollar to settle transactions would probably represent the most severe penalty for targeted enterprises and their governments.

As indicated above, a major advantage of E&F cross-domain responses is that – ideally – it is not necessary to implement official sanctions against these offending enterprises. It could well be sufficient to highlight publically the irresponsible, and even malevolent, space practices made possible by these Chinese and Russian entities doing business worldwide today with total impunity.

As this information is largely open source, it can be publically referenced by the Air Force Space Command, Strategic Command, the State Department, the Pentagon, the National Security Council and/or other podiums.

Conclusion

Addressing the proliferation of unconventional threats to space should be an integral part of the U.S. and allied deterrence. Elevating the risk profile of those offending Chinese, Russian or other companies with exposure to the global markets would, among other penalties, likely damage their corporate reputations/brands, increase their borrowing costs, complicate their access to international capital markets, contract foreign direct investment in their economies, pose corporate governance and possibly compliance problems, spook prospective or existing Western partners and make it harder to prevail in tender bidding processes. These are real world costs – with unsettling knock-on effects – that China and Russia care about deeply, hence the deterrence leverage for the U.S. and its allies. At present, E&F statecraft and this domain's toolkit is rarely, if ever, deployed for the purpose of strengthening space security. This can be changed quickly and for a relatively trivial price-tag.