SQUADRON OFFICER SCHOOL

AIR UNIVERSITY ADVANCED RESEARCH

The Future of Warfare and Russian Engagement in Space

by

Kate E. Lee, Capt, USAF

Advisor: John J. Isacco, Lt Col, USAF

March 2021

Abstract

As technology and warfare have evolved, space-based capabilities and the architecture that enables them have become exponentially more important to national security. Accordingly, space warfare will become a key component of future conflicts. However, current United States (U.S.) and North Atlantic Treaty Organization (NATO) space architecture suffers from poor cybersecurity. Left unaddressed, this will become an unprecedented weakness that adversaries such as Russia can exploit if given the opportunity. Over the next decade, space warfare is likely to be conducted predominantly in the cyber and electronic realms. The biggest threat to U.S. and NATO space architecture will not be from kinetic weapons, but from cyber operators on the other side of the world. This is especially true of the U.S.'s primary challenger in space, Russia. Given Russia's approach to modern warfare, which involves extensive use of non-traditional means, cyberattacks are likely to become Russia's preferred method of warfare in the space domain. The U.S. and NATO therefore need to invest in reinforcing the cybersecurity of their space architecture and develop mandatory cybersecurity standards for implementation in future technologies and assets.

I. Introduction

The Joint Chiefs of Staff have recognized that in the age of technology, "[a]ccess to space is vital to the collective security of the United States and its allies and partners."[i] However, access to space is only as good as the infrastructure that enables it. Current United States (U.S.) and North Atlantic Treaty Organization (NATO) space architecture has a major flaw: poor cybersecurity. This cybersecurity deficit, combined with the U.S. and NATO's near-total dependence on space assets, becomes an unprecedented weakness that adversaries such as Russia can exploit if given the opportunity. The U.S. and NATO should therefore take steps to fortify the cybersecurity of existing space infrastructure and develop cybersecurity standards for implementation in future technologies, as space warfare in the next decade will likely be carried out through non-kinetic means such as electronic and cyber warfare.

II. The Forecast for Space Warfare

Modern nations are incredibly dependent on capabilities provided by their interconnected constellation of space systems, which makes such systems prime high-value targets. By compromising a single space asset, a belligerent actor could gain the ability to impact multiple systems, a threat that is driving the development of various capabilities that can be deployed to counter such a risk.[ii] Current counterspace capabilities fall into one of four categories: kinetic physical, non-kinetic physical, electronic, and cyber.[iii]

Kinetic physical counterspace capabilities refer to weapons that are designed to directly strike or detonate near space assets.[iv] Several nations—the U.S., Russia, China, and India—have successfully developed and tested kinetic counterspace weapons such as direct-ascent anti-satellite (ASAT) and co-orbital ASAT capabilities.[v] However, these weapons are unlikely to be the future of space warfare. Rather, kinetic ASAT capabilities are analogous to nuclear weapons. Possessing and testing them is a show of force that sends a message akin to nuclear deterrence, but much like nuclear weapons, the actual deployment of a kinetic ASAT weapon implicates second- and third- order effects that detract from the system's viability as a practical method of waging war.

While destroying an adversary's satellites or other space assets via kinetic means could undoubtedly provide a strategic advantage, such an attack would come with collateral consequences for all spacefaring nations, to include the aggressor. The use of kinetic ASAT weapons will generate a significant amount of space debris, as evidenced by China's infamous 2007 ASAT test.[vi] China's use of a ballistic missile to destroy one of its defunct satellites resulted in the creation of more than 3,000 pieces of space debris, most of which will remain in orbit for decades.[vii] The build-up of space debris could lead to subsequent collisions between objects, thus creating a chain reaction of collisions and more debris—a phenomenon described as collisional cascading, or the Kessler syndrome.[viii] Not only would this pose an immediate danger to space systems currently in orbit, but it also has long-term implications for the use of space. The scientist who first proposed this possibility, Donald. J. Kessler, hypothesized this could result in the formation of a debris belt around Earth that may render certain orbital ranges unusable for several generations.[ix] Thus, the probability that a kinetic attack's resultant debris could compromise the safety or utility of the belligerent actor's own assets is not insignificant, and will likely serve as a deterrent to the deployment of kinetic ASAT weapons.

The second subset of counterspace capabilities—non-kinetic physical weapons—consist of directed-energy applications such as lasers and high-powered microwave weapons.[x] As with kinetic ASAT capabilities, the world's spacefaring nations have these capabilities in various developmental and operational stages.[xi] To achieve enough power to damage or destroy other space systems, a space-based laser would require a large chemical or solid-state laser, which would then require a large reserve of chemical fuel or electrical power, respectively.[xii] Thus, the practical limitations of existing directed-energy weapons (DEWs) and the technological challenges of proposed space-based DEWs make them unlikely to be mainstays of space warfare, at least for the next few years.

In reality, as will be discussed further below, it is most likely that space warfare in the next decade will be conducted predominantly in the cyber and electronic realms, rather than in the final frontier itself. This will be due in no small part to Russia, the U.S.'s primary challenger in space, and its approach to modern warfare.

III. Expected Russian Activities in the Space Domain

Russia's understanding of war in the modern era is characterized by the use of non-kinetic tools and the concept of "new generation warfare" (NGW), a holistic view of warfare that embraces tools from the entire spectrum of instruments of national power. [xiii] The basic premise of NGW is best summarized by Russia's Chief of the General Staff, General Valery Gerasimov, who noted that: "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[xiv] A good example of Russia's NGW is its own activities in the Ukraine conflict, which involved extensive use of mixed tactics, including political subversion, disinformation, cyberattacks, and last but not least, counterspace capabilities.[xv]

In its 2020 Global Counterspace Capabilities assessment, the Secure World Foundation noted there was "significant evidence that Russia is actively employing counterspace capabilities in current military conflicts."[xvi] Current Russian counterspace capabilities include various kinetic systems, directed-energy weapons, and other tools of electronic and cyber warfare. Russia has tested direct-ascent ASAT missiles intended to intercept targets in low-Earth orbit (LEO) on several occasions.[xvii] Russia has also developed and launched several satellites that have demonstrated the ability to rendezvous with other space objects.[xviii] The maneuvering and rendezvous ability demonstrated by these satellites could be applied to co-orbital ASAT capabilities, such as satellites that are capable of docking and physically interfering with others.[xix] Ultimately, however, a kinetic ASAT capability is unlikely to be Russia's weapon of choice in a near-future space conflict, given Russian leadership's assessment that its conventional military power is inferior to that of the U.S. and NATO, which would make a direct competition of power a losing game.[xx] Further, if there is anything the Kremlin learned from its warfare in Ukraine, it is that open aggression should be avoided, as it will preclude the state from denying responsibility for armed conflict.[xxi] A kinetic counterspace attack would be relatively easy to attribute to a particular actor—using one would paint Russia as an antagonist and draw unwelcome scrutiny.

Another area of significant Russian research and development is directed-energy weapons. In its 2019 statement to the Senate Select Committee on Intelligence, the U.S. intelligence community noted

that "Russia has fielded a ground-based laser weapon, probably intended to blind or damage sensitive space-based optical sensors, such as those used for remote sensing."[xxii] In 2020, the Defense Intelligence Agency advised that Russia is pursuing development of an airborne variant of a laser weapon for use against satellites and mission defense sensors; however, the timeline for operability is unknown.[xxiii,xxiv] Finally, there is no evidence that Russia is pursuing development of a space-based laser ASAT capability at this time.[xxv] Thus, while directed-energy weapons will become a serious threat as the technology matures, they are not expected to be a cornerstone of Russian space strategy in the immediate future.

In light of the above, Russia is likely to favor subtler methods of NGW. While kinetic attacks are easily attributable to a belligerent actor, cyber and electronic warfare (EW), by contrast, are not. Both are essential tools of the Russian military, and their combined application will form the foundation for Russian space warfare. Russia has demonstrated proficiency in EW capabilities such as downlink jamming—interfering with a ground stations' ability to receive transmissions from a satellite—and spoofing, both of which can be used to interfere with an adversary's command and control (C2), communications, and intelligence, surveillance, and reconnaissance (ISR) capabilities.[xxvi] Cyber operations, which have become increasingly central to Russian hybrid warfare, provide another avenue for domineering, degrading, or even destroying adversaries' space assets and associated capabilities.[xxvii] Cyberattacks are likely to become Russia's preferred method of warfare in the space domain, as successful attacks could allow Russia to gain full control of adversaries' satellites and C2 systems from a terminal far, far away, whereas EW may be dependent on proximity to the target asset. The 1998 ROSAT incident, in which Russian hackers hijacked control of a U.S.-German satellite and issued commands that caused the satellite to rotate toward the sun, thereby "frying its optics and rendering it useless," is proof that Russia is willing and able to use cyberattacks against space systems.[xxviii] Russian focus on cyberattacks and large-scale cyber offensives against space assets is especially likely considering the current vulnerabilities of U.S. and NATO space architecture.

IV. Reinforcing Cybersecurity of U.S. and NATO Space Architecture

Given Russia's demonstrated proficiency in NGW, the U.S. and NATO need to make a concerted effort to reinforce the cybersecurity of their space assets, because "[t]oday's systems are not prepared for yesterday's cyber-attacks."[xxix] Despite the fact that space technology has been around for several decades, the current state of cybersecurity for space architecture is abysmal. Because cybersecurity standards for space technology are unregulated, there is a conspicuous gap between current practice and where space cybersecurity needs to be.[xxx]

The exploitation, attack, and denial of space capabilities via cyber operations involves penetration of one or more of the following access points: (1) the satellites, (2) the ground-based infrastructure that supports space-based assets, and (3) the supply chain.[xxxi] In a 2014 study on the cyber defense of space assets, the National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory (JPL) simulated a cyberattack against an approximation of a real-world mission architecture.[xxxii] The architecture was comprised of systems and infrastructure that customarily support space missions and had been "deemed secure by traditional means" such as security checks, vulnerability scans, and configuration management.[xxxiii] The simulation revealed that although cybersecurity coverage for individual systems appeared to be complete, there existed gaps in coverage when the systems were aggregated as a whole.[xxxiv] The combination of systems created "a risk that had never been considered, tested, or accepted" due to the assumption that each individual system was providing the necessary protection.[xxxv]

Considering the historically weak cybersecurity of space assets, it goes without saying that the U.S. and its allies need to evaluate and reinforce the cybersecurity measures for individual components of existing space architecture. JPL's simulation, which identified gaps in the cybersecurity of space assets, also highlights the need for the U.S. and its allies to assess and verify the security of their space architecture as a whole, as it is the combined suite of capabilities—satellites, ground stations, users, and more—that is likely to be the "weakest link." With this in mind, the U.S. and NATO should develop mandatory cybersecurity standards for implementation in future technologies and architectures.

Mandatory standards will provide many benefits, most notably in the supply chain, where they would promote proper vetting of sources and thereby ensure higher quality and more secure products.

The supply chain is an area of concern because it is just as susceptible to cyberattacks as actual space architecture.[xxxvi] Due to the complexity and specialized components required for space assets, the supply chains are as complex as the assets themselves, and with each new vendor comes an additional opportunity for a bad actor to compromise a space asset.[xxxvii] Installing a hidden back door in hardware or software is a prime avenue by which an adversary could compromise a space system from the inside out. To combat the threat posed by third-party components with unknown vulnerabilities or implants, the U.S. and NATO must be highly selective. The Presidential Space Policy Directive 5 states that space system owners and operators "should" adopt cybersecurity practices that align with the National Institute for Standards and Technology (NIST)'s Framework for Improving Critical Infrastructure Cybersecurity.[xxxviii] The suggestion alone is insufficient. Until the promulgation of regulated cybersecurity standards that are specific to space assets, commercial providers of space hardware or software should be required to abide by the NIST framework. This requirement may meet resistance and result in fewer competitors for contracts. However, while leveraging commercial partners is important, it cannot come at the expense of national security. Certain space assets are designed with extremely long lifespans and no system downtime in mind, which can make it difficult to patch or update security after the asset has been put into orbit. Accordingly, the U.S. and its allies need to take every available measure on the front-end to mitigate the cybersecurity risks to their space assets.

V. Conclusion

As technology continues to evolve, so too does the landscape of modern warfare. Space, once the final frontier, is now the latest in which nations will go to war. However, the unique challenges posed by the space environment will drive a different type of warfare, one that is less about kinetic weapons and more about superiority engineered by electronic and cyber means. As proponents of hybrid warfare, Russia is likely to employ electronic and cyber warfare tactics in their attempts to compromise U.S. space assets. Thus, to defend against Russian threats in the short-term, cybersecurity of existing space

architecture must be re-evaluated and reinforced. To endure in the long-term, the U.S. and NATO must develop minimum cybersecurity standards that account for the security of both individual and aggregated space systems. Failure to address the cybersecurity problem in space could put the U.S. behind the curve and have disastrous consequences for U.S. national security.

---

[i] Joint Chiefs of Staff, Space Operations, JP 3-14 (Washington, DC: Joint Chiefs of Staff, 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.
[ii] Gregory Falco, *Job One for Space Force: Space Asset Cybersecurity*, (Cambridge, MA: Harvard Kennedy School, July 2018), 4.
[iii] Todd Harrison, Kaitlyn Johnson, and Makena Young, *Defense Against the Dark Arts in Space* (Washington, DC: Center for Strategic and International Studies, February 2021), 7-9.
[iv] Ibid., 7.
[v]Brian Weeden and Victoria Samson, *Global Counterspace Capabilities: An Open-Source Assessment* (Washington, DC: Secure World Foundation, April 2020), ix-xix.
[vi] Brian Weeden, *2007 Chinese Anti-Satellite Test Fact Sheet* (Washington, DC: Secure World Foundation, November 2010).
[vii] Weeden, *2007 Chinese Anti-Satellite Test Fact Sheet*.
[viii] Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research* 83, no. A6 (June 1978).
[ix] Ibid.
[x] Harrison, Johnson, and Young, *Defense Against the Dark Arts in Space*, 8; U.S. Library of Congress, Congressional Research Service, U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress, by Andrew Feickert. R45098. 2018.
[xi] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment*, ix-xix.
[xii] Ibid., 74.
[xiii] U.S. Library of Congress, Congressional Research Service, *Russian Armed Forces: Military Doctrine and Strategy*, by Andrew S. Bowen. IF11625. 2020.
[xiv] Ibid.
[xv] Ibid.
[xvi] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment*, 51.
[xvii] "Russia Tests Direct-Ascent Anti-Satellite Missile," U.S. Space Command, December 16, 2020, https://www.spacecom.mil/News/Article-Display/Article/2448334/russia-tests-direct-ascent-anti-satellite-missile/; "Russia Tests Direct-Ascent Anti-Satellite Missile," U.S. Space Command, April 15, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2151611/russia-tests-direct-ascent-anti-satellite-missile/.
[xviii] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment*, 54-56.
[xix] Ibid.
[xx] Alina Polyakova et al, *The Evolution of Russian Hybrid Warfare* (Washington, DC: Center for European Policy Analysis, January 28, 2021), 3.
[xxi] Ibid., 13.
[xxii] U.S. Congress, Senate, Select Committee on Intelligence*, Worldwide Threat Assessment of the U.S. Intelligence Committee*, 2019, 17.
[xxiii] Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC, 2019), 29.
[xxiv] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment*, 72-73.
[xxv] Ibid., 74.
[xxvi] Ibid., 67.
[xxvii] Harrison, Johnson, and Young, *Defense Against the Dark Arts in Space*, 20; Polyakova et al, *The Evolution of Russian Hybrid Warfare*, 13.
[xxviii] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment*, 131;

[xxix] DJ Bryne, David Morgan, Kymie Tan, Bryan Johnson, and Chris Dorros, "Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations," *Procedia Computer Science* 28 (2014): 522-530, https://doi.org/10.1016/j.procs.2014.03.064.
[xxx] Gregory Falco, "Cybersecurity Principles for Space Systems," *Journal of Aerospace Information Systems* 16, no. 2 (December 2018): 1-10, https://doi.org/10.2514/1.I010693.
[xxxi] Weeden and Samson, *Global Counterspace Capabilities: An Open-Source Assessment,* 126.
[xxxii] Bryne, Morgan, Tan, Johnson, and Dorros, "Cyber Defense of Space-Based Assets," 525.
[xxxiii] Ibid., 525-527.
[xxxiv] Ibid.
[xxxv] Ibid., 524.
[xxxvi] Beyza Unal, Cybersecurity of NATO'S Space-Based Strategic Assets (London, UK: Royal Institute of International Affairs, July 2019), 7.
[xxxvii] Falco, "Cybersecurity Principles for Space Systems," 2.
[xxxviii] U.S. President, Space Policy Directive 5, "Cybersecurity Principles for Space Systems, Space Policy Directive-5 of September 4, 2020," *Federal Register* 85, no. 176 (September 10, 2020): 56155.