Electronic Warfare in the Space and Cyber Domains

By Richard D. Newbold[1]

"We're in an era of great power competition, and the next major conflict may be won or lost in space. Space is no longer a sanctuary—it is now a warfighting domain."

(Acting) Defense Secretary Patrick M. Shanahan, speaking at the 35th Space Symposium in 2019

Introduction

Electronic warfare (EW)[2] is nearly as old as electronics itself, but the combination of electronic warfare and cyber warfare is more recent and holds the possibility of extending the reach of the enemy into space—a domain that until recently was controlled entirely by only a handful of nation states. Operations in the space domain today are increasingly contested, degraded, and operationally limited,[3] and conflict will inevitably arise.

As the potential for conflict continues to increase, states are developing advanced counterspace capabilities. While the existence of counterspace capabilities is not new, the circumstances have changed. Today, there are increased incentives for development and potential use of offensive counterspace capabilities and greater potential consequences of their widespread deployment, as large parts of the global economy and society are increasingly reliant on space applications.[4]

Space capabilities play an increasingly important role in national security and military operations, and collective reliance on space capabilities makes them a target for adversary counterspace operations.[5] Conflict domains in space include ground-to-space warfare (e.g., attacking satellites from the Earth), space-to-space warfare (e.g., satellites attacking satellites), and space-to-ground warfare (e.g., satellites attacking Earth-based targets). Space assets today face many threats, both natural and man-made,[6] from multiple attack vectors.

Space systems are essential to the critical infrastructure that underpins the global economy and represent a single point of failure for various industries.[7] Virtually every aspect of American national security, including the detection of threats, the use of weapons, and the deployment of forces and their

[1] The author is a former military intelligence systems integrator and Army officer. He supported the National Geospatial-Intelligence Agency intelligence, surveillance, and reconnaissance (ISR) effort as part of Operation Noble Eagle. He also conducted ISR in the Middle East and Southeast Asia for over five years in support of the Army's counterterrorism efforts in the region. Mr. Newbold will be graduating from Georgetown University Law Center in Summer 2020 with an LL.M. in National Security Law. This paper was written to fulfill a requirement for Space Law Seminar (Spring 2020).

[2] Applications of electronic warfare in space include the neutralization of enemy forces, defensive countermeasures, and counter-IED (or the space equivalent). Existing EW technologies adapted for space use include directed energy (DE), electromagnetic pulse (EMP), and cyber (e.g., hacking, command and control disruption).

[3] Joint Publication 3-14, *Space Operations* (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf.

[4] Brian Weeden & V. Samson, *Global Counterspace Capabilities: An Open Source Assessment*, Secure World Foundation, viii (2018), https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[5] Brian Weeden, *Electronic Warfare and Satellites Challenges in Assuring Space Capabilities* (2016), http://swfound.org/media/205651/bw_ew_satellitesatellites-gcc_oct2016.pdf.

[6] Weeden, *supra* note 3, at I-6.

[7] Gregory Falco, *The Vacuum of Space Cybersecurity*, Conference Paper, 2 (2018), https://www.researchgate.net/publication/327678396.

resupply, is dependent on the integrity of critical space-based capabilities.[8] Over the past several decades, continuous improvements in technology, the transfer of technology, and globalization of services has led to the development and proliferation of advanced space systems across the commercial, civil, and military sectors.[9]

Electronic warfare capabilities are useful in war but, like any weapon in a nation's arsenal, they are only appropriate in certain situations. Although the United States currently enjoys significant overmatch in the space domain, adversaries are challenging that overmatch by creatively avoiding traditional U.S. strengths, thus allowing them to achieve their objectives despite U.S. military dominance in traditional warfare domains.[10] Similar to air, land, and maritime operations, space operations and assets are interconnected with cyberspace through the electromagnetic spectrum (EMS),[11] which today permeates every warfighting domain.

"Cyberspace" is a global domain within the information environment consisting of an interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[12] The common definition of "space" places it 62 miles above Earth's mean sea level.[13] To the extent that the two domains intersect, electronic warfare may be waged in both space and cyberspace simultaneously and at times may cross from one domain to the other.

This paper will discuss electronic warfare usage against enemy space targets and the justification for the use of cyber electronic warfare against assets bound for outer space. It will also discuss applicable law and policy and cite examples of EW and cyber operations in the space context. While the use of cyber warfare or electronic warfare is legal in certain contexts, the fields are developing so quickly that few states can act or respond in sophisticated or nuanced ways. Further, the non-attributive nature of cyberwarfare makes it difficult to determine when a state has acted at all, let alone determine whether the state was justified or acted with hostile intent.

I. Background and Historical Context

Some nations and corporations view space as the next frontier to be exploited but forget that outposts on the perimeter are often resource intensive and difficult to protect. At its height, the Roman Empire stretched from the Atlantic Ocean all the way to the Euphrates River. With such a vast territory to govern, the empire faced an administrative and logistical nightmare. The Romans were unable to communicate quickly or effectively enough to manage their holdings and struggled to marshal enough troops and resources to defend the frontiers from outside attacks. More and more funds were funneled

[8] Lawrence Sellin, *The U.S. is Unprepared for Space Cyberwarfare*, Military Times (2019), https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/.
[9] JP 3-14, *supra* note 3.
[10] Joint Chiefs of Staff, *Cross-Domain Synergy in Joint Operations Planner's Guide*, 1 (2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230.
[11] JP 3-14, *supra* note 3, at I-3.
[12] Computer Security Resource Center, *Cyberspace* (2020), https://csrc.nist.gov/glossary/term/cyberspace.
[13] According to NOAA, a common definition of space is known as the Kármán Line, an imaginary boundary 100 kilometers (62 miles) above mean sea level. In theory, once this 100 km line is crossed, the atmosphere becomes too thin to provide enough lift for conventional aircraft to maintain flight. At this altitude, a conventional plane would need to reach orbital velocity or risk falling back to Earth. See https://www.nesdis.noaa.gov/content/where-space.

into the military for empire upkeep as technological advancement slowed and Rome's civil infrastructure fell into disrepair.[14] This scenario is one to keep in mind as U.S. influence (military or otherwise) expands into the far reaches of the universe while relying on aging infrastructure that is increasingly subject to attack from not only established rogue actors but also emerging asymmetric threat actors. The overall state of U.S. national security is impacted by its many component elements, to include space security and cybersecurity. The question today is whether America's cyber-centurions can adequately protect the farthest reaches of America's expanding space empire.

a. National Security

The concept of national security describes the relationship between capabilities a nation has developed and the challenges posed by the environment in which it must operate. Security involves the task of overcoming both man-made and natural threats in the extreme hostility of the space environment. The behavior of all space-faring entities inevitably affects the security of others. When a country is secure, it enjoys the ability to conduct activities free from harm.[15] As the importance of space grows, national security is increasingly tied to space security.

b. Space Security

Space security is the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction. By this definition, all actors have enjoyed a high level of space security for most of the Space Age. However, challenges to space security are increasing as space becomes more crowded.[16] For its part, the military anticipates space threats on the horizon and is also preparing to prevent and manage future conflicts.[17] The U.S. should actively work with the international community to develop international rules and laws that safeguard space and manage space traffic. In addition, by making satellite systems less vulnerable to attack, and by providing diplomatic structures for conflict resolution, the U.S. can reduce the risk that conflicts in space might lead to conflicts on the ground.[18]

c. Cybersecurity

Cybersecurity is the "art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[19] Cybersecurity and space security are inextricably linked. Vulnerabilities at the junction of cybersecurity and space-based or space-derived capabilities cause major national, regional, and international security concerns that are going mostly unaddressed, apart from some high-end space-based systems. Analyzing

[14] Evan Andrews, *Eight Reasons Why Rome Fell*, History.com (2014), https://www.history.com/news/8-reasons-why-rome-fell.

[15] James Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*, 11 (2nd ed, 2011), ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/georgetown/detail.action?docID=744004.

[16] *Id.* at 11.

[17] On this perspective, see John Hyten, *A Sea of Peace or a Theater of War? Dealing with the Inevitable Conflict in Space* (1999), https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/Hyten.pdf.

[18] *Space Security*, Union of Concerned Scientists (2014), https://www.ucsusa.org/resources/space-security.

[19] Security Tip (ST04-001), *What is Cybersecurity?*, CISA, https://www.us-cert.gov/ncas/tips/ST04-001

the intersection between cyber and space security is essential to understanding this non-traditional, evolving security threat.[20]

d. Evolution of Electronic Warfare

Electronic warfare has evolved over time as have space capabilities. As the name implies, "electronic" warfare requires electronics, which began with the invention of the vacuum diode by J.A. Fleming, in 1897, followed by the vacuum triode used to amplify electrical signals.[21] Since the beginning of the 20th century, radio pioneers recognized the military application of the electromagnetic spectrum. During World War II, British forces used radio transmissions to overpower German radio receivers. The jamming missions successfully disrupted German command and control systems and navigation capabilities.[22] In the decades that followed, state and non-state actors alike used radios to support navigation, command and control, intelligence gathering, and information operations,[23] a state practice which continues today, especially in the context of land warfare. As we will see, many land warfare concepts, practices, and capabilities that have been battle tested over time are now being adapted to the space environment.

e. Cold War Developments

During the Cold War (1947-1991), the behavior of the Soviet Union and the United States dominated space security considerations as the two sides conducted more than 95 percent of space activities.[24] During this period, outer space utilization was primarily for strategic operations such as strategic intelligence gathering, nuclear attack early warnings, and execution of arms control agreements.[25] This scenario has changed in the meantime, and space today has a far more important role to play in conventional military operations.[26] Today, balance-of-power dynamics are impacting outer space, which has become yet another domain where terrestrial politics and competition play out.[27]

For the U.S. and Soviet Union, achieving space security was for many years primarily a matter of understanding the policies of the other side and attempting to reach consensus on how to best manage disputes while also preventing hostile acts. With the collapse of the Soviet Union and end of the Cold War in 1991, space became mainly the realm of the U.S. For the decade following, Washington continued its policy of negotiated space security in close cooperation with the Russian Federation.[28]

---

[20] David Livingstone & Patricia Lewis, *Space, the Final Frontier for Cybersecurity?*, Chatham House (2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[21] Electronics Projects Focus, *Brief History of Electronics and Its Development* (2020), https://www.elprocus.com/know-about-brief-history-of-electronics-and-their-generations/.

[22] ATP 3-12.3, *Electronic Warfare Techniques* (2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18105_ATP%203-12x3%20FINAL%20WEB.pdf.

[23] *Id*. at 1-1.

[24] Moltz, *supra* note 15, at 11.

[25] Weeden, s*upra* note 4.

[26] Rajeswari Rajagopalan, *Electronic and Cyber Warfare in Outer Space*, United Nations Institute for Disarmament Research, 3 (2019), https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

[27] *Id*. at 4.

[28] Moltz, *supra* note 15, at 12.

f. Dependency and Vulnerability

Many countries today utilize space for more than simple military advantage. Offensive or defensive counterspace operations today would impact not just the security sector but also social and economic sectors across the continents due to large-scale civilian dependency on space-based applications. The fact that space is vital to both civilian and military operations heightens the danger of inadvertent escalation and conflict.[29] [30] The advent of the Internet has introduced both opportunity and risk. Because the Internet is based on a globally shared infrastructure, if the U.S. government conducts a cyberattack against a foreign enemy, the blowback effects threaten domestic entities[31] as well as assets abroad, even extending into space.

Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack an enemy.[32] While space equipment today is electronic warfare hardened[33] to the extent plausible, older satellites and electronic objects were launched (or otherwise placed into space) without much consideration for cybersecurity. For context, the Internet did not even exist when Vangard 1—still in orbit—was launched by the U.S. Navy in 1958.[34] The next section will explore warfare in the space domain, which shares many of the characteristics of the other traditional domains of land, air, and maritime.

II. Warfare in the Space Domain

DoD space forces are the space and terrestrial systems, equipment, facilities, organizations, and personnel that conduct space operations. Space systems consist of three related segments: ground,[35] link,[36] and space.[37] Space operations impact or utilize space-based assets to enhance the potential of the U.S. and multinational partners.[38] Many states today are approaching space from a security perspective, relying on outer space to strengthen strategic and national security capabilities.[39]

Challenging a space adversary may involve denying that adversary freedom of action. While the notion of denying freedom of action may appear to conflict with other legal obligations regarding the right of passage and allowance of freedom of action, the key word is "adversary." DoD further specifies the

[29] If there is, for instance, a disruption or denial of service during a period of heightened tensions, even if the incident was a natural incident or due to mechanical failure.
[30] Rajagopalan, *supra* note 26, at 3.
[31] William A. Owens et al., Committee on Offensive Information Warfare, National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 38 (2009)
[32] Joint Publication 3-13.1, *Information Operations*, (2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.
[33] Radiation hardening is the process of making electronic components and circuits resistant to damage or malfunction caused by high levels of ionizing radiation (particle radiation and high-energy electromagnetic radiation), especially for outer space.
[34] NASA Space Science Data Coordinated Archive, *Vanguard 1* (2020), https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1958-002B.
[35] The ground segment consists of ground-based facilities and equipment supporting command and control (C2) of space segment resources, as well as ground-based processing equipment, Earth terminals or user equipment, space situational awareness (SSA) sensors, and the interconnectivity between the facilities in which this equipment is housed.
[36] The link segment consists of signals connecting ground and space segments through the electromagnetic spectrum.
[37] The space segment involves the operational spacecraft within the space joint operating area (SJOA), which lies in the space domain.
[38] JP 3-14, s*upra* note 3, at I-2.
[39] Rajagopalan, *supra* note 26, at 4.

military will intervene "when directed."[40] In other words, a space-faring party at some point may be determined to be an adversary, and DoD personnel may be directed at that time to deny this adversary freedom of movement. However, until deemed an adversary, the U.S. allows the space systems of all nations to enjoy the rights of passage through space without interference, and purposeful interference with space systems, to include supporting infrastructure, would be considered an infringement of a nation's rights.[41]

a. Challenges of Operating in Space

Like the air, land, and maritime domains, space is a physical domain within which military, civil, and commercial activities are conducted.[42] The space domain is the "area above the altitude where atmospheric effects on airborne objects become negligible." Conducting warfare in space is technically challenging and requires persistent precision over a vast physical area.[43]

Space is a naturally hazardous environment and is increasingly congested, contested, and competitive.[44] It is here that the military seeks to achieve space control, defined as "[o]perations to ensure freedom of action in space for the United States and its allies and deny an adversary freedom of action in space."[45] The purpose of these operations is to achieve space superiority[46] without prohibitive interference.

Achievement of space control in such a remote and rugged domain requires effective tools, and electronic warfare is often the tool of choice due to its unique characteristics. Mostly invisible to the naked eye and often measurable only with specialized instruments, the effects may be seen only after the fact.

b. Counterspace Capabilities

Counterspace capabilities deprive an adversary of the benefits of space capabilities.[47] Some analysts stipulate that they involve anything that precludes an adversary from exploiting space to his advantage.[48] These capabilities enable a space power to maintain "a desired degree of space superiority

[40] JP 3-14, *supra* note 3, at I-3. "U.S. space forces conduct space control operations to ensure freedom of action in space for the U.S. and its allies and, *when directed* [emphasis added], to deny an adversary freedom of action in space."

[41] Jimmy Carter, Presidential Directive/NSC-37, *National Space Policy*, ¶1.d (1978) ("The space systems of any nation are national property and have the right of passage through and operations in space without interference. Purposeful interference with operational space systems shall be viewed as an infringement upon sovereign rights."). Available at https://www.hq.nasa.gov/office/pao/History/nsc-37.html.

[42] JP 3-14, *supra* note 3, at vii.

[43] JP 3-14, *supra* note 3.

[44] JP 3-14, *supra* note 3, at viii.

[45] JP 3-14, *supra* note 3, at GL-6.

[46] The Jan. 2020 release of the *DOD Dictionary of Military and Associated Terms* defines "space superiority as" "The degree of control in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from terrestrial or space-based threats." Available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[47] Air Force Doctrine Document 2-2.1, *Counterspace Operations* (2004), https://fas.org/irp/doddir/usaf/afdd2_2-1.pdf.

[48] J.B. Sheldon, *Threats to Security in Space from Counter-Space Technologies*, ASEAN Regional Space Security Workshop, Hoi An, Vietnam, (2012), http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Workshop%20on%20Space%20Security,%20Hoi%20An,%206-7December2012/Annex%205%20-%20Space%20Security.pdf.

by the destruction or neutralization of enemy forces."[49] Categories of counterspace technologies include kinetic, non-kinetic, and electronic warfare.

The emergence of electronic and cyber counterspace capabilities is enabling a wider range of actors, (both state and non-state) to target and disrupt space objects, including both military and civilian satellites. These capabilities are already being used to target objects both in space and on the terrestrial battlefield.[50]

Broadly speaking, counterspace capabilities (including an EW element) can be used to create temporary or permanent destruction of space assets. States are moving away from expensive anti-satellite (ASAT) options toward development of more affordable and readily available electronic and cyber warfare methods. While kinetic systems create permanent and irreversible destruction of space assets, electronic and cyber means have thus far created mostly disruptions and damage to space systems of a temporary nature.[51]

c. Advantage Through Asymmetry

Regional and global security competition is a driver for a space arms race as major spacefaring powers seek new military space capabilities.[52] Other states have recognized the asymmetric advantage that U.S. forces gain from space and are implementing military strategies designed to deprive the U.S. of its advantage. [53] The possibility of impacting multiple systems by compromising a single space system makes certain targets attractive from a military standpoint. Space assets, including both ground systems and satellites, are fundamental underlying components of much of the nation's critical infrastructure,[54] [55] and there appears to be a greater willingness to engage in the development and possible use of new offensive counterspace capabilities. Indeed, competition between major space powers has led to a rise in the number of instances where electronic and cyber warfare capabilities are used.[56]

d. State Actor Threats

China conducted successful antisatellite missile tests in 2007[57] and 2014,[58] and Chinese military writings emphasize the necessity of "destroying, damaging, and interfering with the enemy's reconnaissance . . .

---

[49] *Air Force Basic Doctrine*, *Volume 1* (2015), https://www.doctrine.af.mil/Portals/61/documents/Volume_1/Volume-1-Basic-Doctrine.pdf.

[50] Rajagopalan, *supra* note 26, at 1.

[51] *Id.*

[52] Rajagopalan, *supra* note 26, at 4.

[53] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 14-15 (2015), http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power _Report.pdf.

[54] Critical infrastructure is described by the Department of Homeland Security as 16 different sectors that seem discreet yet have many commonalities across them. For example, most critical infrastructure relies on space systems.

[55] Gregory Falco, *The Vacuum of Space Cybersecurity*, Conference Paper, 1 (2018), https://www.researchgate.net/publication/327678396.

[56] Rajagopalan, *supra* note 26, at 4.

[57] Moltz, *supra* note 15, at 26. While also serving other purposes, the Feb. 2008 U.S. ASAT shot may have been intended in part as a "signal" from administration proponents of such a view to the Chinese military regarding U.S. resolve.

[58] Colin Clark, *Chinese ASAT Test Was 'Successful': Lt. Gen. Raymond*, BreakingDefense (2015), http://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/; and Leonard David, *China's Anti-satellite Test: Worrisome Debris Cloud Circles Earth*, Space.com (2007), http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

and communications satellites."[59] Chinese actions in no way endeared the nation to the international space community, as large debris fields from the worst debris-generating event in the history of the Space Age[60] will remain with us for the indefinite future.

In 2014, Chinese hackers attacked National Oceanic and Atmospheric Administration (NOAA), the federal weather network, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping, and other crucial uses. NOAA makes satellite data and imagery publicly available through the Internet,[61] which immediately opened up the agency to rogue actors from around the globe. Weather satellites orbit hundreds to thousands of miles above Earth and offer continuous views of weather systems, such as hurricanes, thunderstorms, and cold fronts while measuring temperature and moisture at different altitudes. All this data is necessary for prediction modeling on a global scale, so the agency was a prized hack at the time. NOAA characterized its decision to cut off satellite images as causing minimal disruption but had previously touted those same systems as intrinsic to the nation's environmental intelligence.[62] The ability of the Chinese to exploit U.S. vulnerabilities in this and other cases helped to bolster support for an increase in cyber funding and put an even stronger spotlight on U.S. cybersecurity initiatives.

North Korea is also considered a rogue terrestrial actor with space aspirations. The North insists its space program is purely scientific in nature, but the U.S., South Korea, and even China say rocket launches are aimed at developing intercontinental ballistic missiles.[63] In February 2013, North Korea set off a nuclear test yielding an explosion roughly the size of the bomb that leveled Hiroshima, Japan. Just days later, the Pentagon announced an expansion of its force of anti-missile interceptors in California and Alaska and began to unveil its "left of launch" program to disable missiles prior to launch. Gen. Martin Dempsey, then Chairman of the Joint Chiefs of Staff, announced the program, saying that "cyberwarfare, directed energy, and electronic attack"[64] were all becoming important new adjuncts to the traditional ways of deflecting enemy strikes.

In 2014, after DoD stepped up cyber and electronic strikes against North Korea's missile program in hopes of sabotaging test launches in their opening seconds, a large number of its military rockets did begin to explode, veer off course, disintegrate in midair, and crash into the sea.[65] While the North Korean rockets were not intended for space, per se, an intercontinental ballistic missile capable of traveling along a suborbital trajectory halfway around the world may have been viewed by U.S. officials as a threat and worthy of intervention by means of electronic and cyber warfare. Electronic warfare advocates believe that the targeted attacks gave U.S. anti-missile defenses a new edge and delayed by

---

[59] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 14-15 (2015), http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power _Report.pdf

[60] Frank Morring Jr., *Worst Ever: Chinese anti-satellite test boosted space-debris population by 10% in an instant*, Aviation Week and Space Technology, 20 (2007).

[61] Weather radar data can be accessed at https://www.weather.gov/Radar.

[62] Mary Flaherty, et al., *Chinese Hack U.S. Weather Systems, Satellite Network*, Wash. Post (2014), https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

[63] *North Korea Fires Long-Range Rocket Despite Warnings*, BBC News (2016), https://www.bbc.com/news/world-asia-35515207

[64] Unlike electronic attacks that interfere with the transmission of radiofrequency signals, cyberattacks target the data itself and the systems that use this data.

[65] David E. Sanger & William J. Broad, *Trump Inherits Secret Cyberwar with N. Korea*, N.Y. Times, A07 (2017), https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

several years the day when North Korea would be able to threaten U.S. cities with nuclear weapons atop intercontinental ballistic missiles.[66]

e. Significance of Satellites

Satellites are important for military and other applications because they allow users to view large areas of the Earth at once. This ability means satellites can collect more data more quickly than instruments on the ground. Also, satellites also can peer into space better than telescopes on Earth's surface. Because satellites fly above the clouds, dust and molecules in the atmosphere that would normally block the view from the ground level do not interfere.[67]

Some of the norms that have existed are being challenged because newer actors seem less bound by them. While the norm to not test ASATs is rarely breached, there are indications that other norms, such as non-interference in satellite operations, is weakening. Norms are likely to be broken when so many new players enter an already established field. Norms can be effective when players are committed to upholding the rules but break down when the rules become a hindrance to maintaining advantage. The erosion of norms is further aided by changes in technology and political context, like the widespread availability of cyber warfare technologies combined with a heightened sense of competition driven by geopolitics.[68]

Satellites are operated by personnel on the ground who send commands to a spacecraft via an electronic uplink. If this command uplink were to be successfully attacked electronically, a satellite would be rendered useless either immediately or over time.[69] Computer code transmitted directly to satellites in orbit could potentially allow remote control of a system, preventing access to onboard sensors and communications systems. Adversaries could similarly enter ground control systems and issue alternative instructions to satellites to move them out of position or shut off critical systems.[70] All of this could be accomplished without putting personnel in harm's way, clearly an advantage militarily speaking.

Because of the importance of satellites, antisatellite electronic jammers capable of degrading the use of Global Positioning System (GPS) satellites for precision navigation and strike and communications satellites are readily available.[71] Jammers targeting the downlink from GPS satellites prevent users from receiving accurate and useful precision navigation and timing information from the spacecraft. These vulnerabilities exist because satellites are basically sophisticated drones flying about in space.[72]

Natural threats to satellites include solar activity, radiation belts, and natural orbital debris. Manmade threats can be both unintentional (e.g., debris or electromagnetic interference) or intentional (e.g.,

---

[66] *Id*.

[67] Brian Dunbar, *What is a Satellite?* (2014), https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-a-satellite-58.html.

[68] Rajagopalan, *supra* note 26, at 4.

[69] E. Lincoln Bonner, *Defending Our Satellites: The Need for Electronic Warfare Education and Training*, 79 (2015), https://www.afspc.af.mil/Portals/3/documents/Schreiver%20Essay%202019/2015_SEW-Bonner.pdf.

[70] Catherine A. Theohary & John R. Hoehn, *Convergence of Cyberspace Operations and Electronic Warfare*, Congressional Research Service (2019). https://crsreports.congress.gov/product/pdf/IF/IF11292.

[71] Cited in Brian Garino & Jane Gibson, *Space System Threats*, AU-18, Space Primer, prepared by Air Command and Staff College Space Research Electives Seminars, 276 (2009), http://aupress.maxwell.af.mil/digital/pdf/book/AU-18.pdf; and cited in Dewitt Morgan, Space Power: A Critical Strength . . . and a Critical Vulnerability of the US Military, 11 (2007).

[72] Bonner, s*upra* note 69, at 79.

jamming, lasing, cyberattack, and ASAT).[73] The protection of U.S. satellites will likely depend on the military's ability to conduct successful EW operations to jam and strike adversary counterspace network sensors, which are generally large immobile facilities. Because of this, tactical systems[74] to electronically locate sensors are usually not necessary, although today's large facilities will likely become smaller and more mobile over time. As this evolution occurs, the conduct of successful electronic warfare operations to locate and jam mobile systems and companion counterspace strike batteries will become both more important and more challenging.[75]

Military ground forces are and will continue to be vulnerable in present and future conflicts due to a dangerous reliance on satellite communication (SATCOM) and a degraded readiness to fight in the face of a growing counterspace and communications EW threat. Although SATCOM provides significant advantages over terrestrial communication systems, it carries liabilities for which the military is largely unprepared. The increasing need for SATCOM bandwidth has led the military to channel its operational communications through leased networks of commercial satellites that lack adequate protection against jamming and are susceptible to state-actor influence. Potential adversaries such as the Russian Federation and the People's Republic of China have long recognized U.S. dependence on SATCOM and have developed formidable capabilities to attack that dependence. In addition to manmade SATCOM threats, periodic geomagnetic storms can damage satellites in orbit.[76] Because of their significance, all satellites require protection, and certain satellites must be protected at all cost.

III. Electronic Warfare

DoD defines electronic warfare as a "[m]ilitary action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[77] [78] Electronic warfare can be described as military action involving the use of directed energy to control the electromagnetic spectrum, to deceive or attack an enemy, or to protect friendly systems from similar actions. EW uses focused energy such as radio waves or laser light to confuse or disable enemy electronics.[79] Historically, electronic warfare has played significant roles in combat operations,[80] and this will continue to be the case in the context of space.

Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies.[81] The most common type of electronic warfare

[73] JP 3-14, *supra* note 3, at vii-viii.

[74] The High-speed Anti-Radiation Missile (HARM) Targeting System, or HTS is an example of a tactical system. See https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104602/high-speed-anti-radiation-missile-targeting-system/.

[75] Bonner, *supra* note 69, at 78.

[76] Andrew H. Boyd, *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army* (2017), https://www.ausa.org/publications/satellite-and-ground-communication-systems-space-and-electronic-warfare-threats-united.

[77] *DOD Dictionary of Military and Associated Terms*, 71 (2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[78] Michael Lilienthal personal correspondence, *EW Paper Comments* (2020). Electronic warfare expert Michael Lilienthal has noted the definition of electronic warfare does not include cyber warfare.

[79] JP 3-13.1, s*upra* note 32.

[80] ATP 3-12.3 *supra* note 22, at 1-1 (2019).

[81] Air Force Doctrine Document 2-5, *Information Operations*, 5 (2005), https://apps.dtic.mil/dtic/tr/fulltext/u2/b311353.pdf.

are jamming[82] and eavesdropping, which is part of intelligence gathering and has grown in relative significance due to the increased technical complexity of modern warfare.[83] The spectrum is the common denominator for both cyberspace and electronic warfare operations, which suggests that independent approaches to securing information networks may leave vulnerabilities for adversaries to exploit in either cyberspace or in the electromagnetic spectrum.[84]

a. Near-Peer Threats

Peer adversaries such as Russia and China continue to develop new technologies capable of complex computer network and electronic warfare operations. U.S. forces understand how their assets are vulnerable to these capabilities and, conversely, how similar capabilities may be employed against adversarial systems.[85] Electronic and cyberwarfare may be the preferred ways to attack space capabilities, because they do not have the same long-term consequences as kinetic attacks (e.g., space debris).[86] Aside from enjoying an overall smaller footprint than a division of tanks rolling into battle, for example, cyber electronic warfare activities are often not attributable to the cyber actor. The ability to physically destroy an object with an invisible ray of energy combined with some lines of code makes the combination of EW and cyber extremely efficient and potent.

Cyber and electronic warfare threats should be contextualized together to create the most effective defense but also to inspire a discourse on developing the most effective offense.[87] The relationship between space and cyberspace is unique in that many space operations depend on cyberspace, and a critical portion of cyberspace can only be provided via space operations.[88] Many states today rely on outer space for military communications, and a greater dependence on outer space for military operations leaves states vulnerable to a range of counterspace operations. [89]

b. Governance

Military cyberspace operations use cyber capabilities to create effects that support missions in both physical domains and in cyberspace.[90] Cyberspace operations (CO) is the "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[91] Cyberspace operations are described by DoD as the military, intelligence, and ordinary business operations of the DoD in and through cyberspace.[92] At the senior military level, the priority is to establish an effective governance structure to coordinate a multiservice approach to harmonizing electromagnetic spectrum and cyber activities and doctrines in addition to overseeing new investments in offensive and defensive technologies to support these efforts. The U.S. government, and DoD in

[82] Jamming falls under the category of electronic countermeasures (ECM). It limits an enemy's ability to exchange information by overriding radio transmissions or by sending signals to prevent radar detection or convey false information.
[83] Encyclopaedia Britannica, *Electronic Warfare* (2017), https://www.britannica.com/topic/electronic-warfare.
[84] Sam Cohen, *Integrating Cyber and Electronic Warfare*, The Cyber Edge (2018), https://www.afcea.org/content/integrating-cyber-and-electronic-warfare.
[85] *Id*.
[86] Weeden, *supra* note 3.
[87] Cohen, s*upra* note 84.
[88] JP 3-14, *supra* note 3, at I-2
[89] Rajagopalan, *supra* note 26, at 4.
[90] Theohary & Hoehn, *supra* note 70.
[91] Joint Publication 3-12, *Cyber Operations*, vii (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[92] Theohary & Hoehn, *supra* note 70.

particular, recognize that the synchronization of cyber and electronic warfare is key for U.S. forces to succeed. Experts predict that high-end peer conflict will not be won by merely leveraging electromagnetic spectrum use (such as utilizing space-based satellites) to provide global communications, surveillance, missile warning, or position navigation but rather will be won by projecting control from within the spectrum itself.[93]

In 2017, Congress mandated the Secretary of Defense "establish processes and procedures to integrate strategic information operations and cyber-enabled information operations" and "ensure that such processes and procedures provide for integrated Defense-wide strategy, planning, and budgeting with respect to the conduct of such operations by the Department, including activities conducted to counter and deter such operations by malign actors."[94] The concept of global space governance is not well defined at the intergovernmental level, but DoD is clearly exercising its strength domestically in combination with National Aeronautics and Space Administration (NASA) and other civilian space actors.

IV. Space Law

The term "space law" refers to a body of law drawn from a variety of sources and consisting of two basic types of law governing space-related activities: international and domestic. The former refers to rights and obligations the U.S. has agreed to through multilateral or bilateral treaties and agreements. The latter refers to domestic legislation by Congress and regulations promulgated by federal executive agencies.[95]

a. International

Space law is a developing field of law with a relatively short history going back to the 1950s following rapid technological developments of World War II.[96] International space law derives from several sources, including maritime law, air law, treaty law, and UN legislation.[97] In this sense, the law of outer space is not a wholly coherent set of rules and practices.[98] Sources of international space law are primarily found in international legal rules and international custom with general principles filling the gaps in the absence of exclusive sources.[99]

The international space law framework has three components: the general regime of space law; laws governing certain space applications; and declarations. The body of treaty law negotiated among states within the United Nations framework includes principles regarding exploration activities, astronaut rescue, and space object liability.[100] The second important component of international space law

[93] Cohen, *supra* note 84.

[94] National Defense Authorization Act for Fiscal Year 2018, *House Conference Report to Accompany H.R. 2810* (2017), https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf.

[95] Jane Gibson & Jeremy Powell, *Current Space Law and Policy Report*, AU-18 Space Primer Report, Air Command and Staff College and Space Research Electives Seminars (2009). https://www.jstor.org/stable/resrep13939.10.

[96] Atsuyo Ito, *Legal Aspects of Satellite Remote Sensing*, 17 (2011).

[97] *Id*. at 20.

[98] Francis Lyall & Paul B. Larsen, *Space Law: At Treatise*, 449 (2nd ed., 2018).

[99] See C.J. Cheng, New Sources of International Space Law, *The Use of Air and Outer Space Cooperation and Competition: Proceedings of the International Conference on Air and Outer Space at the Service of World Peace and Prosperity*, Held in Beijing from Aug. 21-23 1995, Kluwer Law International, The Hague-Boston-London, 1998, 215.

[100] See Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Oct. 27, 1967, 610 UNTS 205; Agreement on the Rescue of Astronauts, the Return of Astronauts and

governs certain applications such as satellites.[101] The third international space law component includes declarations on outer space exploration and use.[102]

The U.S. is a party to certain treaties that address space activities[103] that can be categorized into three types: scientific, military, and commercial.[104] Activities involving electronic warfare fall primarily into the military category, although there are commercial applications of EW-related activities which would also fall into the commercial category.

Law of war treaties and the customary law of war are understood to regulate the conduct of hostilities, regardless of where they are conducted, which would include the conduct of hostilities in outer space. In this way, the application of the law of war to activities in outer space is the same as its application to activities in other environments, such as the land, sea, air, and cyber domains.[105] Outer space may be viewed as somewhat analogous to the high seas[106] in that no state may claim sovereignty over outer space,[107] and space systems of all nations have rights of passage through space without interference.[108]

Both space law and general international law (including International Humanitarian Law, or IHL) place restrictions on the use of weapons in outer space.[109] One of the underlying principles of space law is that space will be used for "peaceful purposes." This principle can be found in both the United Nations

---

the Return of Objects Launched Into Outer Space (1968), 672 UNTS 199; Convention on International Liability for Damage Caused by Space Objects, Nov. 29, 1971 24 UST 2389; Convention on Registration of Objects Launched Into Outer Space, Nov. 12, 1974 28 UST 695.; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, (1979) 18 ILM 1434.

[101] See Principles Relating to Remote Sensing of the Earth from Outer Space (1986), UNGA Resolution 47/68 on the Principles relevant to the Use of Nuclear Power Sources in Outer Space, adopted on Dec. 14, 1992.

[102] See UNGA Resolution 1962 (XVIII) on Declaration of Legal Principles Governing the Activities of States in exploration and Use of Outer Space, adopted on Dec. 13, 1963; and UNGA Resolution 51/122 on Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries, adopted Dec. 13, 1996.

[103] Outer Space Treaty, art. VI ("States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty.").

[104] Ito, *supra* note 96, at 23.

[105] *Department of Defense Law of War Manual* (2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

[106] Arthur J. Goldberg, U.S. Ambassador to the United Nations, *Treaty on Outer Space: Hearings Before the Committee on Foreign Relations*, U.S. Senate, 90th Congress, First Session, 63 (1967) ("This is an attempt, once we leave airspace, and get to outer space, however you define the limits, this is an attempt to create in outer space the closest analogy and that is the high seas.").

[107] Outer Space Treaty, art. II ("Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.").

[108] See, e.g., Outer Space Treaty, art. I ("Outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."); National Space Policy of the United States of America, 3 (2010).

[109] P.J. Blount, *Targeting in Outer Space: Legal Aspects of Operational Military Actions in Space*, Harv. Nat'l. Sec. J. (2012), https://harvardnsj.org/wp-content/uploads/sites/13/2012/11/Targeting-in-Outer-Space-Blount-Final.pdf.

General Assembly resolution on the legal principles applicable to outer space[110] and in the Outer Space Treaty.[111]

b. United Nations Charter

Law as an aggregate of human conduct requires harmonization of institutions.[112] Provisions in the UN Charter on the general use of force are relevant because the charter states "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." This would then include any and all use force and aggression in outer space under the UN Charter mandate.

Article 51 of the UN Charter deals with the right to individual or collective self-defense in the case of an armed attack. There are ongoing debates on the right to self-defense and what should be classified as an act of aggression. Article 51 provides in part that "[n]othing in the Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." The inherent right of self-defense of Article 51 remains the major justification for the maintenance of armed forces by states throughout the world.[113]

The UN Charter, then, bans the use of aggressive force but allows for self-defense and Security Council-sanctioned use of force.[114] Lawful military activities in self-defense (e.g., missile early warning, use of weapon systems) would be consistent with the use of space for peaceful purposes, but aggressive activities that violate the UN Charter would not be permissible.[115]

c. Outer Space Treaty

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (referred to as Outer Space Treaty, or OST) is the foundational treaty regulating outer space activities.[116] The scope of the Outer Space Treaty consists of the nature of space activities, the subjects conducting space activities, and the applicability of other international law to the treaty.[117]

---

[110] Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, G.A. Res. 1962 (XVIII), U.N. Doc. A/RES/1962(XVIII) (1963).

[111] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205. Available at http://www.unoosa.org/pdf/publications/STSPACE11E.pdf.

[112] Charles C. Okolie, *International Law of Satellite and Remote Sensing*, 151 (1989).

[113] Lyall & Larsen, *supra* note 98, at 451.

[114] Refer to § 14.10.3 (Outer Space Treaty Restrictions on Military Activities).

[115] Q. Christol Carl, *The International Law of Outer Space*, 114 (1966) ("It may be concluded that both ballistic missiles, directly, and satellites, indirectly, have military utility. This does not automatically exclude them from the category of peaceful uses, since defensive and deterrent capabilities serve the cause of peace. It is only when such devices are intentionally used for aggressive purposes that they lose their peaceful status.").

[116] Refer to § 14.10.3 (Outer Space Treaty Restrictions on Military Activities).

[117] Ito, *supra* note 96, at 23.

Much of the content of the OST had been agreed upon in the UN General Assembly Resolutions International Co-operation in the Peaceful Uses of Outer Space[118] and the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space.[119] The OST imposes restrictions on certain military operations in outer space in that it does not exempt military spacecraft or military space activities from its purview.[120]

Article III of the Outer Space Treaty incorporates the Charter of the United Nations into the space law regime[121] and quotes the UN Charter by declaring that the treaty's purpose is to promote "international peace and security."[122] The OST also reaffirms the duty of states to comply with existing international law in carrying out activities in outer space. Article III further provides that "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding."[123] This means that the laws of *jus ad bellum* and *jus in bello* would also apply in space. However, there is no guidance on how such laws should be applied, and it is unclear what provocation would justify the destruction of a satellite or space object as a "proportionate" response.[124]

Article IV does not establish prohibitions with respect to weapons that are not weapons of mass destruction (e.g., anti-satellite laser weapons or other conventional weapons).[125] Article IV provides that "[t]he moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes."[126] Article IV also places certain prohibitions on military activities on the moon and other celestial bodies such as establishment of military bases, installations, and fortifications; testing of any type of weapons; and conduct of military maneuvers.[127] It should be noted that these activities are prohibited only on the moon and other celestial bodies, not in outer space itself,[128] and that space assets capable of conducting EW would likely be in orbit or mounted to another craft that is in orbit.

---

[118] United Nations Office for Outer Space Affairs, *General Assemble Resolution 1721 (XVI)*, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/resolutions/res_16_1721.html.

[119] United Nations Office for Outer Space Affairs, *Resolution 1962 (XVIII)*, https://www.unoosa.org/oosa/oosadoc/data/resolutions/1963/general_assembly_18th_session/res_1962_xviii.html.

[120] Refer to § 14.10.3 (Outer Space Treaty Restrictions on Military Activities).

[121] Outer Space Treaty, art. III.

[122] *Id*.

[123] *Id*. See also Staff Report prepared for the use of the Committee on Aeronautical and Space Sciences, United States Senate, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies: Analysis and Background Data, 24 (1967) ("This article makes clear that those nations which ratify the treaty will observe international law—and this includes the Charter of the United Nations—in order to promote international cooperation and peace. Thus that body of law, which has developed on the Earth in order to bring about harmonious relations between nations and settle disputes without resort to violence, would become applicable to outer space, the Moon, and other celestial bodies.").

[124] UNIDIR, *An Update on "Outer Space Security" and a Brief History of the Prevention of an Arms Race in Outer Space* (2018), https://www.unidir.org/files/medias/pdfs/presentation-to-inform-cd-subsidiary-body-3-discussion-eng-0-778.pdf.

[125] David A. Koplow, *ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons*, 30, Mich. J. Int'l L. 1187, 1198 (2009) ("This provision does not impede the stationing of non-nuclear weapons (including conventional ASAT weapons) in space, nor does it affect a nuclear weapon that makes only a temporary transit of outer space, as when propelled by an intercontinental ballistic missile (ICBM) toward its target, rather than being 'stationed' in space.").

[126] Outer Space Treaty, art. IV ("The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes.").

[127] Outer Space Treaty, art. IV ("The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden.").

[128] Law of War, s*upra* note 105.

Article IX is pertinent to the debates on noninterference in the peaceful activities of state parties. If a party to the treaty believes an activity or experiment would cause potentially harmful interference in the peaceful exploration and use of outer space, it is required to undertake appropriate international consultations before proceeding. If a party engaged in a certain activity which might cause harmful interference does not establish consultations, then the affected party has a right to ask for consultation.[129] To the extent that non-state actors might participate in electronic warfare, the Outer Space Treaty provides for state responsibility for the activities of nongovernmental entities in outer space.[130]

V. Cyber, Space, and Electronic Warfare Policy

Policy differs from law in a few respects. Policy can be easier to create but is often less permanent as in the case of executive action in the form of proclamations, orders, directives, and memoranda. When the subsequent chief executive is sworn in, it is possible that four or eight years of work could disappear with the stroke of a pen. Generally, however, if a policy is working well, the executive actions carry over to the next administration and may even be incorporated into statute or treaty, making them less subject to the political whims of opposing parties.

a. Domestic Policies

In March 2005, the National Defense Strategy identified cyberspace as a new theater of operations.[131] Also in 2005, the Air Force mission statement expanded to reflect that cyberspace was an official Air Force domain: "to fly and fight in air, space, and cyberspace."[132]

The 2010 National Space Policy reiterated that all nations have the right to explore and use space for peaceful purposes and for the benefit of all humanity, in accordance with international law. Consistent with this principle, "peaceful purposes" allows space to be used for national and homeland security activities. The U.S. employs a variety of measures to help assure the use of space for all responsible

[129] The relevant portion of Article IX states in full "If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State Party to the Treaty which has reason to believe that an activity or experiment planned by another State Party in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, may request consultation concerning the activity or experiment."

[130] Outer Space Treaty, art. VI ("States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty.").

[131] George W. Bush, *The National Defense Strategy of the United States of America* (2005). https://archive.defense.gov/news/Mar2005/d20050318nds1.pdf.

[132] C. Todd Lopez, *Cyber Summit Begins at Pentagon Nov. 16*, A.F. Print News (2006), http://www.af.mil/news/story.asp?id=123032005.

parties, will deter others from interference and attack, and will defend its space systems and defeat efforts to attack them.[133]

The National Space Policy recognizes a right "consistent with the inherent right of self-defense, [to] deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and , if deterrence fails, defeat efforts to attack them."[134] DoD space policy is likewise intended to deter adversaries, defend against threats, and pursue resilient space architectures that contribute to achieving space mission assurance and objectives.[135]

Sustained space access is vital to the collective security of the U.S. and its allies. In accordance with the 2017 National Security Strategy, the United States considers unfettered freedom to operate in space to be a vital interest and warns that and any harmful interference with critical components of its space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of its choosing.[136]

b. International Regulations and Standards

It is the policy of the U.S. government to protect U.S. global access to the radiofrequency spectrum and related orbital assignments required to support the use of space. The U.S. identifies impacts to government space systems prior to reallocation of spectrum for commercial and federal. It also identifies sources of radio frequency interference and take necessary measures to sustain the radiofrequency environment in which critical U.S. space systems operate.[137]

The International Telecommunication Union (ITU), a United Nations agency, regulates frequencies of satellite communications to prevent communication interference and registers the orbit of satellites, but there are few standards beyond these areas.[138] A special characteristic of telecommunication satellites is that they use radio frequencies for transmission, which is why ITU frequency spectrum management is so critical.[139] Unfortunately, regulation of satellites is generally weak. There are no agencies that restrict the use of satellites, and there is no overarching governing body that monitors the specific use of satellites. Even if one did exist, there are no mechanisms for enforcing treaties, standards, or governance.[140]

The Radio Regulations of the ITU are the basic documents that, along with the ITU Constitution and Convention, enunciate the main principles and specific regulations for the registration of satellite network frequency assignments. The regulations, revised partially or fully in exceptional circumstances, form a binding treaty in governing the radiocommunication and orbital frequencies. They are meant to

---

[133] Barack H. Obama, *National Space Policy of the United States of America* (2010) https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.

[134] *Id.*

[135] JP 3-14, s*upra* note 3, at I-1.

[136] Donald J. Trump, *National Security Strategy of the United States of America* (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[137] Obama, *supra* note 133.

[138] International Telecommunications Union, *ITU Radio Regulatory Framework for Space Services* (2016), https://www.itu.int/en/ITU-R/space/snl/Documents/ITU-Space_reg.pdf.

[139] P.P.C. Haanappel, *The Law and Policy of Air Space and Outer Space*, 137 (2003).

[140] Gregory Falco, *The Vacuum of Space Cybersecurity*, Conference Paper, 3 (2018), https://www.researchgate.net/publication/327678396.

be the foundation in ensuring an interference-free or interference-controlled environment for satellite operations.[141]

Recognizing the sovereign right of each state over its telecommunication, the ITU is concerned with maintenance and extension of cooperation regarding the use of telecommunication on the international plane. Article 48 (military exemption) of the ITU Constitution provides that "[m]ember States retain their entire freedom with regard to military radio installations," a provision that the Experts Group agreed reflects longstanding state practice with respect to the governance of international telecommunications.[142]

In an effort to shape policy, the U.S. participates in a number of standards bodies and also supports nongovernmental organizations (NGO) whose views align with national policy goals. We have already identified several laws and policies applicable to electronic warfare in both space and cyber. We will now discuss an application in the case of directed energy weapons, an important tool of electronic warfare.

VI. Directed Energy Weapons

"Directed energy" is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.[143] Directed energy weapons (DEW) can amplify or disrupt an electromagnetic field, resulting in the jamming, overpowering, and deceiving of information managed by computerized systems or electronic platforms such as surveillance or telecommunication satellites.[144] Sometimes this form of attack is temporary with no physical damage because, after a jammer is turned off, communications return to normal.[145]A directed-energy weapon damages a target with highly focused energy, including laser, microwave, or particle beams. These electromagnetic systems convert chemical or electrical energy to radiated energy and focus it on a target, resulting in physical damage that degrades, neutralizes, defeats, or destroys adversarial capabilities.[146] These weapons overheat the electric circuitry of almost any piece of equipment, whether electronic or not, resulting in the destruction or interference of a machine's electrical-based functions and components.[147]

Lasers are a type of directed energy weapons that destroy or disable mechanized devices through creation of intense heat.[148] Potential applications of these weapons include targeting of personnel, missiles, vehicles, and optical devices. Some scholars argue the presence of DEW in space endangers the lives of satellites and other peaceful space objects such as space stations and shuttles. They further

---

[141] Rajagopalan, *supra* note 26, at 14.

[142] Louis de Gouyon Matignonh, *Article 48 of the ITU Constitution*, Space Legal Issues (2019), https://www.spacelegalissues.com/article-48-of-the-itu-constitution/.

[143] JP 3-13.1, *supra* note 32.

[144] Cohen, *supra* note 84.

[145] Todd Harrison, *Space Threat Assessment 2019*, CSIS, 4, (2019), https://www.csis.org/analysis/space-threat-assessment-2019.

[146] Peter Morrison, Office of Naval Research, *Directed Energy Weapons: Counter Directed Energy Weapons and High Energy Lasers*, https://www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-science-research-351/directed-energy-weapons-cdew-and-high-energy-lasers.

[147] Cohen, *supra* note 84.

[148] Using the world's most powerful x-ray laser, physicists have heated matter to 3.6 million degrees Fahrenheit.

argue that deployment of a directed energy laser in space for the purpose of destroying the property of another is an act of aggression and possibly even an act of war.[149]

The defense industry has argued there must be ways to harness the power of a discriminate laser weapon within the Law of Armed Conflict and to continue developing technology that can target adversarial weapon systems and defend against missiles.[150] Targeting a missile from space with a laser requires high beam quality, adaptive optics, and advanced pointing control to steer the laser beam as it is transmitted through the atmosphere—technology that is costly and requires a high degree of sophistication.[151]

Proponents argue that DEW expands the menu of response options and may result in better decision making and outcomes. They point out that flight time is less of a consideration because the energy beam travels at the speed of light. The technology therefore enables better decision making, because there is more time to identify a target and then fire, whereas a kinetic interceptor would require any response to account for flight time toward the missile. Another DEW advantage is that the weapons can be reused to fire as many times as their power systems allow. A further benefit, fewer satellites are required for missile defense if armed with directed energy weapons rather than kinetic interceptors.[152] Another advantage in the view of some proponents, certain directed energy weapons have the potential to circumvent existing legal restrictions and prohibitions on weapons, such as the prohibition on blinding laser weapons, creating comparable effects to prohibited systems but not falling within their technical definitions. In addition to equipment, space-based weapons could also target personnel,[153] raising additional legal questions related to the avoidance of unnecessary suffering.[154]

Traditional interpretations of protective principles, including the prohibition on causing superfluous injury or unnecessary suffering to combatants may be challenged by novel ways of inflicting physical and mental harm. Historically, systems that harmed subjects through non-kinetic means had often been considered an issue of concern and requiring special consideration. There appears to be little publicly available data and considerable uncertainty about the environmental and health effects of directed energy weapons,[155] but certainly such weapons are designed to create stress on the body which would manifest in elevated heartrate and body temperature, at a minimum, if directed at a human target.

---

[149] Okolie, *supra* note 112, at 192.

[150] Robert Ward, *The Dawn of Anti-Personnel Directed-Energy Weapons*, RealClear Defense (2018), https://www.realcleardefense.com/articles/2018/07/24/the_dawn_of_anti-personnel_directed-energy_weapons_113641.html.

[151] Brian Garino & Jane Gibson, *Space System Threats*, AU-18 Space Primer, 277 (2009), http://space.au.af.mil/au-18-2009/au-18_chap21.pdf.

[152] Jon Harper, *Special Report: The Pentagon Could Put Directed Energy Weapons in Space* (2019), https://www.nationaldefensemagazine.org/articles/2019/4/25/special-report-the-pentagon-could-put-directed-energy-weapons-in-space.

[153] Article36 Discussion Paper, *Directed Energy Weapons* (2017), http://www.article36.org/wp-content/uploads/2017/11/DEW-Final-17Nov17.pdf.

[154] The principle that weapons causing unnecessary suffering must be avoided is set forth in the Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land of Oct. 18, 1907. The Annex to the Convention: Regulations respecting the laws and customs of war on land - Section II : Hostilities - Chapter I : Means of injuring the enemy, sieges, and bombardments - Regulations: Art. 23, subparagraph (e) refers to "arms, projectiles, or material calculated to cause unnecessary suffering." See https://ihl-databases.icrc.org/ihl/WebART/195-200033?OpenDocument.

[155] Article36, s*upra* note 153, at 5.

Air Force medical researcher Lt. Col. Richard Yoo of the Counter Directed Energy Weapons Branch in the Air Force Medical Support Agency was quoted in 2017 as saying "We're in the early stages of learning about the long- and short-term medical affects these weapons have on people, both in terms of collateral damage and users." He further stated that "Directed energy weapons are definitely part of the future of warfighting."[156]

The use of weapons in outer space is regulated by the 1967 Outer Space Treaty, which states that all use of outer space must be in accordance with international law. The prospect of DEW raises questions under several bodies of international law, most notably those that place restrictions on the use of force. Some DEW are classified as "non-lethal" or "less-lethal" weapons, with proponents distinguishing them from "lethal" weapons. DEW that are designed to deliver an electromagnetic blast or to target satellites raise concerns due to their potential impact on civilian infrastructure.[157]

Civilian infrastructure in space today is minimal but growing as more players enter the field. For example, China's State Council first mentioned the development of a private space industry in 2014, pledging at that time to "encourage private capital's participation in China's construction of civilian space infrastructure." Since then, military-civilian partnerships have flourished, and private firms have been allowed to launch from Chinese military bases.[158] In reaction to the perceived threat, Acting Defense Secretary Patrick Shanahan bluntly asserted in 2019 that China was "deploying directed energy weapons," and had "weaponized space with the intent to hold American space capabilities at risk."[159]

All prospective weapons undergo a legal review during development and prior to acquisition to ensure that the weapon or munition in question complies with U.S. international legal obligations. No specific rule prohibits laser weapons. In fact, antipersonnel weapons are designed specifically to kill or disable enemy combatants and are not unlawful because they cause death, disability, pain, or suffering. This principle is tempered by law of war obligations relating to the legality of weapons or munitions contained in the Annex to Hague Convention IV Respecting the Laws and Customs of War on Land.[160] The DoD position has been consistent for decades after it concluded in 1988 that lasers as antipersonnel weapons do not cause unnecessary suffering nor otherwise constitute a violation of U.S. international legal obligations and that lasers as antipersonnel weapon are lawful.[161]

Important questions remain about how restrictions and prohibitions that could apply to DEW under IHL would apply to their use in outer space.[162] Because the law has evolved as a result of military experience, it is designed to be applied in time of armed conflict. In no areas does use of directed enemy

---

[156] Peter Holstein, *Directed energy weapons research a new frontier for Air Force Medicine*, *Air Force Medical Service* (2017), https://www.airforcemedicine.af.mil/News/Display/Article/1365970/directed-energy-weapons-research-a-new-frontier-for-air-force-medicine/.

[157] Article36, s*upra* note 153, at 6.

[158] Charlie Campbell, *From Satellites to the Moon and Mars, China Is Quickly Becoming a Space Superpower*, Time (2019), https://time.com/5623537/china-space/.

[159] Theresa Hitchens, *Shanahan: China Is Deploying Directed Energy Weapons*, BreakingDefense (2019), https://breakingdefense.com/2019/04/shanahan-china-is-deploying-directed-energy-weapons/.

[160] Article 23(e) prohibits the employment of arms, projectiles, or material calculated to cause unnecessary suffering. There is no internationally accepted definition of unnecessary suffering. In fact, an anomaly exists in that while it is legally permissible to kill an enemy soldier, in theory any wounding should not be calculated or intended to cause unnecessary suffering.

[161] Louise Doswald-Beck, Blinding Weapons: Reports of the meetings of experts convened by the International Committee of the Red Cross on Battlefield Laser Weapons 1989-1991, Geneva, International Committee of the Red Cross, Annex C, 367-371 (1993).

[162] Article36, *supra* note 153, at 6.

weapons conflict with the principles of war, such as maintenance of momentum, concentration of effort, surprise, etc.[163]

VII. Thwarting Threats from a Rogue Regime

In 2018, there was an escalating threat on the Korean peninsula, and there was speculation that the U.S. military may have intervened to disrupt one or even several attempted North Korean rocket launches. Probably only a small number of military planners know what actually happened, but let us assume that rocket and nuclear development continued to the point where the North was capable of launching a nuclear weapon the same rocket and announced to the world it was exercising treaty rights, sovereignty, and freedom of movement by putting a peaceful non-nuclear satellite into orbit. In turn, the U.S. administration, on December 15, 2019, in consultation with Congress, conducted a simultaneous electronic warfare attack from both land and space, resulting in the death of one North Korean military member who was hit in Wonsan, North Korea by falling shrapnel from a disintegrating rocket. U.S. Navy SEALs were able to heroically recover an intact nuclear device—not a satellite as previously stated by a North Korean spokesman—which had fallen harmlessly in the Sea of Japan. Subsequent media reports indicated the U.S. had hacked into North Korean launch and command and control systems and also used space-based assets to interfere with or destroy North Korean military infrastructure critical to a successful launch.

a. Threat of Imminent Attack

The text of Article 51 of the U.N Charter refers to the right of self-defense "if an armed attack occurs against a Member of the United Nations."[164] Under customary international law, states had, and continue to have, the right to take measures to respond to imminent attacks.[165] A U.S. president would also have authority to respond to an imminent threat arising from his constitutional responsibility to protect the nation.[166] In our scenario, Congress had already authorized the use of all necessary and appropriate military force against North Korea. It could be argued that the threat was not actually imminent, however, since the Korean conflict which began in 1950 was still technically ongoing at the time of the cyber and electronic warfare attack. However, a more specific threat came when North Korea threatened the U.S. in early December 2019 with an unwelcomed "Christmas gift."[167] Such threats

---

[163] International Committee of the Red Cross, *The Law of Armed Conflict*, 7-1 (2002), https://www.icrc.org/en/doc/assets/files/other/law1_final.pdf.

[164] U.N. Charter, art. 51.

[165] Lord Peter Henry Goldsmith, Attorney General, United Kingdom, Oral Answers to Questions, Apr. 21, 2004, Hansard 660 House of Commons Debates §§ 370-71 ("It is argued by some that the language of Article 51 provides for a right of self-defense only in response to an actual armed attack. However, it has been the consistent position of successive United Kingdom Governments over many years that the right of self-defense under international law includes the right to use force where an armed attack is imminent. The language of Article 51 was not intended to create a new right of self-defense. Article 51 recognizes the inherent right of self-defense that states enjoy under international law. … It is not a new invention. The charter did not therefore affect the scope of the right of self-defense existing at that time in customary international law, which included the right to use force in anticipation of an imminent armed attack.").

[166] John Yoo, *The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them*, Memorandum Opinion for the Deputy Counsel to the President (2001), https://fas.org/irp/agency/doj/olc092501.html.

[167] Simon Denyer, *North Korea Warns United States of an Unwelcome "Christmas Gift,"* Wash. Post (2019). The Christmas gift may also have been referring to cyberattack. In May 2018, the FBI and DHS issued a technical alert notifying the public about the FBI's high confidence that malicious North Korean government cyber actors had been using malware since at least 2009 to target multiple victims globally and in the United States, across various sectors, including critical infrastructure sectors.

in combination with U.S. intelligence were enough to convince the President that the U.S. could refrain no longer.

Such a U.S.-led operation against North Korean as described in our scenario would comply with the four fundamental law of war principles governing the use of force: necessity, distinction, proportionality, and humanity.[168] Under the principle of necessity, a basic tenet of international law is that attacks against civilians are prohibited. If the U.S. had attacked North Korea's civilian airline reservation system instead of a military rocket launch pad, the operational commander would have had a difficult time justifying this action under the test of military necessity. Attacks, for example, against the country's financial, transportation, or communications systems would have to have demonstrated clear military necessity to be legal.[169]

An attack must be necessary for a military purpose, and the damage it causes must be worth the advantage that is gained.[170] It would be consistent with these principles to continue an operation if anticipated civilian casualties would not be excessive in relation to the anticipated military advantage.[171] In this case, the U.S. was careful in its planning, and there were no civilian casualties. The rule of distinction states "The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians."[172] This attack meets the criteria, as it was directed specifically against military assets.

The rule of proportionality states that "Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited."[173] Under the principle of proportionality, it is reasonably clear to a military campaign planner which target is legal if the choice is between a military rocket or a baby milk factory. When the attack will indiscriminately affect huge sectors of the enemy's economy for an unknown amount of military advantage, the commander must ask difficult questions as to its legality. Weapons that are incapable of being controlled (that is, directed at a military target) are forbidden as being indiscriminate in their effect.[174] Military experts have long proposed a "surgical strike,"[175] against North Korea, and this limited controlled U.S. attack potentially prevented nuclear war, saving tens of thousands of lives. The principle of humanity forbids the infliction of all suffering, injury, or destruction not necessary for achieving the legitimate purpose of a conflict.[176] In this analysis, the legitimate purpose of the conflict was to prevent an imminent threat in the form of a North Korean nuclear launch, and that effort was successful.

---

[168] See United States Air Force, *Targeting*, Air Force Doctrine Document 2-1.9, 88 (2006); Dinstein, *Conduct of Hostilities* at 16-20, 115-16, 119-23.

[169] Karl Kuschner, *Legal and Practical Constraints on Information Warfare*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/kuschner.pdf.

[170] *Id*. at 3.

[171] Chairman of the Joint Chiefs of Staff Instruction 5810.01D, *Implementation of the DoD Law of War Program*, 1 (2020).

[172] International Humanitarian Law, Rule 1, *The Principle of Distinction between Civilians and Combatants Related Practice*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1.

[173] The principle of proportionality in attack is codified in Article 51(5)(b) of Additional Protocol I and repeated in Article 57. See https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14.

[174] Kuschner, *supra* note 169.

[175] Gregory Keeley, *It's Time to Use Surgical Strikes, Naval Blockades and More on North Korea*, TheHill, (2017), https://thehill.com/opinion/national-security/363050-its-time-to-use-surgical-strikes-naval-blockades-and-more-on-north.

[176] The "laws of humanity" are referred to in the St. Petersburg Declaration of 1868, and in what is now known as the Martens Clause derived from the preamble to Convention (IV) respecting the Laws and Customs of War on Land, adopted by the 1907 International Peace Conference at The Hague. Legal recognition of crimes against humanity originated in the jurisprudence of the

b. Anticipatory Self-Defense

Anticipatory self-defense is a response in anticipation of an attack.[177] It must be in "response to an imminent threat of armed attack"[178] and must be proportionate to the threat.[179] Excessive use of retaliatory force is illegal, and states may be held responsible for disproportionate use of force.[180] Anticipatory self-defense often corresponds with the standard established in the famous 1837 Caroline case.[181] It could be argued that not only were thousands of lives saved by blowing up a North Korean rocket, but this action was necessary given the rapid development of the technology employed and the increasing geographic range of the tests.

When determining the legitimacy of a pre-strike action, both historical practice and statutory interpretation can influence the analysis. The restrictive school of interpretation believes that the language requires an attack to occur before one state can legitimately use force against another. But less restrictive arguments hold that a state need not wait until an armed attack has occurred to launch a legitimate pre-attack strike. This view leans on the weight of the "inherent right" of self-defense to argue that a state should be permitted to act to defend its citizens when it believes an attack is impending.[182]

c. Treaties and International Legal Obligations

The Law of Armed Conflict (LOAC) is comprised of both customary law and treaties. Customary law applies to all states. As far as treaties are concerned, they are binding only upon contracting parties.[183] North Korea is not a signatory to the Outer Space Treaty,[184] no obligation to abide by its terms,[185] and is not liable for any legal ramifications if found in violation of any OST articles. Article 34, the General Rule Regarding Third States, of the Vienna Convention on the law of treaties confirms that "[a] treaty does not create either obligations or rights for a third State without its consent.[186]

Nuremberg Tribunal; such acts also constitute a category of crime in the 1998 Rome Statute of the International Criminal Court. Brownlie states that humanity is a source of international law. He cites as a classic reference the judgment in the Corfu Channel case (I.C.J. Reports 1949, 22): the court relied on certain "general and well recognized principles", including "elementary considerations of humanity, even more exacting in peace than in war". I. Brownlie, *Principles of Public International Law*, Clarendon Press, Oxford, 28 (1998).

[177] Lyall & Larsen, *supra* note 98, at 451-452.

[178] *Case Concerning Military and Para-Military Activities in and against Nicaragua (Nicaragua v. United States)* (Merits), Judgement, 1986 ICJ Rep, 14 at 102-4 (paras 193-5) 1986 25 ILM 1023.

[179] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Jurisdiction and Admissibility, Judgment, I.C.J. Rep., 94 (1984).

[180] I.M. Vasilogeorgi, *Military Uses of Outer Space: Legal Limitations, Contemporary Perspectives* (2014) *39 J. Sp. L.* 416.

[181] In that case, British soldiers in Canada crossed the Niagara River to attack and send over Niagara Falls the American steamship Caroline that was assisting Canadian rebels. The British asserted that they attacked in self-defense, but then-Secretary of State Daniel Webster wrote in correspondence with the British government in 1842 that the use of force prior to suffering an attack qualifies as legitimate self-defense only when the need to act is "instant, overwhelming, and leaving no choice of means, and no moment for deliberation."

[182] Alex Potcovaru, *The International Law of Anticipatory Self-Defense and U.S. Options in North Korea*, Lawfare (2017), https://www.lawfareblog.com/international-law-anticipatory-self-defense-and-us-options-north-korea.

[183] Yoram Dinstein, et al., *Oslo Manual on Select Problems of the Law of Armed Conflict: Rules and Commentaries*, 5 (2020).

[184] *Supra* note 111.

[185] Steven Mirmina personal correspondence, *North Korea and the Outer Space Treaty* (2020).

[186] *Vienna Convention on the Law of Treaties (with Annex)*, Concluded at Vienna on May 23, 1969. https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf.

Outer space is to be used for peaceful purposes only. Most Western nations, including the United States, equate peaceful purposes with nonaggressive ones. Consequently, all nonaggressive military use of space is permissible, except for specific prohibitions of certain activities noted elsewhere. North Korea had been escalating threats toward the United States in years leading up to the December 2019 strike as its nuclear program had progressed. The U.S. responded by conducting a congressionally authorized operation against North Korea and acted in national self-defense to protect U.S. persons and interests who were under continual threat of violent attack by North Korean operatives planning operations against them.

To defend its actions for a pre-strike attack on North Korea, the U.S. could make a substantial legal argument based on international law and case precedent. The threat of a rogue state with a weapon of mass destruction (WMD) casts a degree of unpredictability on how states, fearful but constrained, would react. But the variability of historical examples and the behavior of United Nations Security Council members make it unclear what degree of legitimacy the international community would afford the U.S. decision.[187]

Under the U.N. Charter, the Security Council has the sole ability to authorize the use of force against a state. If a state fails to receive this authorization but makes a pre-strike attack regardless, claims of self-defense will face much closer scrutiny[188] China and Russia have both shown willingness to support the North Korean regime in various ways, and their veto power over such a resolution could prevent such a U.S.-proposed measure from being passed. In this case, the U.S. would likely have asserted that North Korea posed an imminent threat as per its understanding of Article 51 of the U.N. Charter[189] and launched a preemptive strike. Article 2(4) forbids states from engaging in the threat or use of force against each other. Yet Article 51 says that the charter does not prohibit the "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[190]

The U.S. could argue that the North Koreans' previous development of an intercontinental ballistic missile (ICBM) (in conjunction with a nuclear warhead small enough to arm that missile) presented an existential threat to Americans' well-being and could have destabilizing global geopolitical effects. The U.S. could further seek the authority of a Security Council resolution, in which case the legal question of an imminent threat would fall, as preventive force authorized by the U.N. Security Council is legal.[191]

Under a series of Security Council resolutions, North Korea is prohibited from developing both nuclear weapons and ballistic-missile technologies. United Nation's Resolution 1718[192] expresses the UN's "firm conviction" that the international regime on the non-proliferation of nuclear weapons be maintained and recalls that North Korea cannot have the status of a nuclear-weapon state in accordance with the Treaty on the Non-Proliferation of Nuclear Weapons. This resolution stemmed from national security concerns related to threats sent by North Korea to South Korea, the U.S., and other nations. Although

[187] Potcovaru, *supra* note 182.
[188] *Id.*
[189] The U.S. view is that any violation of the threat of use of force is a violation of Article 51.
[190] Potcovaru, *supra* note 182.
[191] *Id.*
[192] United Nations Security Council Resolution 1718 (2006), https://www.undocs.org/S/RES/1718%20(2006).

the resolution was adopted in 2006, North Korea is still widely regarded as a rogue nation known for projecting itself as a powerful country through violence and threats.[193]

North Korea's satellite launch, as that nation described it, would fall within Outer Space Treaty legal parameters. If the nation's satellite narrative were true, launching a satellite into orbit to survey land, for example, would be a peaceful action. Article III of the Treaty articulates, "Parties to the Treaty shall carry on activities in the exploration and use of outer space…in the interest of maintaining international peace and security and promoting international co-operation and understanding."[194] North Korea, on the other hand, along with Iran are irrational destabilizing regimes that "might value the destruction of an adversary's space asset over preservation of their own."[195]

To the extent that activities leading up to the U.S. operation against North Korea may have included espionage activities, Article 24 of the Annex to the 1907 Hague Convention IV recognizes the lawfulness of espionage during armed conflict, specifically providing that "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[196] International conventions have not addressed the legality of peacetime espionage, and espionage has been practiced by states for centuries. International law does not prohibit espionage as a fundamentally wrongful activity. [197]

Under LOAC, two types of attacks against civilians are prohibited: 1) direct and deliberate attacks; and 2) indiscriminate attacks. According to the Protocol I in Article 51(2) of the Geneva Conventions, "[t]he civilian population as such, as well as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread the terror among the civilian population are prohibited."[198] In our case, civilians were not directly or deliberately targeted (or injured), and the attack was categorically and geographically limited and not indiscriminate in its intent or execution.

---

[193] United Nations Security Council Resolution 1718 was adopted unanimously by the United Nations Security Council on Oct. 14, 2006.

[194] United Nations Office for Outer Space Affairs, 2222 (XXI) *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

[195] P.J. Blount, *Renovating Space: The Future of International Space Law*, 40 Denv. J. Intl'l L. & Pol'y, 515, 520 (2011).

[196] Convention Respecting the Laws and Customs of War on Land, and its annex: Regulation Concerning the Laws and Customs of War on Land, art. 24, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.

[197] Roger D. Scott, Territorially Intrusive Intelligence Collection and International Law, 46 A.F. L. Rev. 217, 218 (1999).

[198] See Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(3), June 8, 1977, 1125 U.N.T.S. 3; Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, Part IV, Dec. 12, 1977, 1125 U.N.T.S. 609. The United States has not ratified these Protocols, however, the Protocols are recognized by many foreign countries as customary International Law. See Michael J. Matheson, The United States' Position on the Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions, U.J. International Law and Policy, 419, 420 (1987) (identifying specific military conducts in the war zone that insulate a military personnel from being charged with a war crime); see also the Int'l Comm. of the Red Cross [ICRC], Protection of Civilian Population Against the Dangers of Indiscriminate Warfare, ICRC Res. XXVIII (1965) (unsuccessfully attempted to prohibit use of high altitude bombing on the account of excessive collateral damage).

d. Cyber Versus Traditional Kinetic Response

Precisely how the law of war applies to cyber operations is not well-settled as new cyber capabilities are developed and states determine their views in response to such developments.[199] Specific law of war rules may apply to cyber operations, even though these rules were developed long before cyber operations were even possible.[200]

The modern lexicon considers all types of online intrusions to be cyberattacks, although many commentators assert that such indiscriminate use of the term "cyberattack" is incorrect. The National Research Council's 2009 report[201] on cyberattack capabilities defines the term as "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks." The NRC Report distinguishes between cyberattacks, which are destructive in nature, and "cyber exploitations," which are non-destructive actions that extract confidential information.[202]

Cyberattacks are providing an increasingly attractive alternative to direct kinetic operations and may be part of a multifaceted approach that includes diplomacy and economic assistance. The changing nature of warfare has enhanced the attractions of inflicting the damage of war by non-kinetic means. The techniques of cyberwar are a subset of a broader approach to national defense technology that involves the use of the electromagnetic spectrum.[203] That is not to say that cyberattacks cannot inflict significant physical damage to equipment or personnel.[204] If the physical consequences of a cyberattack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyberattack would equally be subject to the same rules that apply to attacks using bombs or missiles.[205]

---

[199] Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. Naval War College International Law Studies, 459, 464-65 (2002) ("The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations. … Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.").

[200] *Law of War*, *supra* note 105, at 1013.

[201] Owens et al., *supra* note 31.

[202] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech., 415.

[203] Claire O. Finkelstein & Kevin H. Govern, *Introduction: Cyber and the Changing Face of War*, Faculty Scholarship. Paper 1566 (2015), http://scholarship.law.upenn.edu/faculty_scholarship/1566.

[204] A notable example, Stuxnet was a malicious computer worm first discovered in 2010 that targets supervisory control and data acquisition (SCADA) systems. Stuxnet is believed to have been responsible for causing substantial damage to the nuclear program of Iran. *Infosecurity* notes several additional examples involving hospital ventilators, oil pipelines, trains, steel plants, and the electrical grid. https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/.

[205] Harold H. Koh, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (2012), reprinted in 54 Harv. Int'l L.J., 3-4 (2012) ("In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced

Arguably, a cyberattack that causes physical damage might constitute an armed attack under Article 51. In our case, the cyber operation resulted in the death of one North Korean military member who was hit by falling rocket shrapnel. While the military member was not the target of the attack, he was in physical proximity to the target of the attack (the rocket) and became collateral damage.

One could argue that non-lethal forms of warfare do constitute the "use of force," and therefore would not be subject to the laws of armed conflict. To advance that contention, proponents must demonstrate that these actions are legal under peacetime international laws. This would be a difficult task, as international law would consider such acts illegal in peacetime, hence they must be measured against the principles of the laws of warfare.[206]

Annihilation of a military computer network could be categorized as a proper military objective. This cyber warfare operation in our scenario resulted in the same outcome as using precision guided missiles to target specific military buildings without the resulting collateral damage to surrounding civilian infrastructure. With proper intelligence gathering and operational planning, the U.S. avoided networks dedicated solely to medical facilities. If not, the attacks may have been deemed to be indiscriminate.[207]

Cyber operations may present issues under the law of war governing the resort to force (i.e., *jus ad bellum*). A cyber operation may in certain circumstances constitute a use of force within the meaning of Article 2(4) and customary international law.[208] Article 2(4) of the Charter of the United Nations states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[209] If cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that trigger a nuclear plant meltdown; open a dam above a populated area, causing destruction; or disable air traffic control services, resulting in airplane crashes.[210]

Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibitions on the resort to force.[211] Offensive cyber operations may violate U.S. international legal obligations, including potential violations of sovereignty, the principle of non-intervention, and the prohibition on the threat or use of force. To the extent an offensive cyber operation (e.g., inserting malware into a rocket launch system) does violate international law, the wrongfulness of that operation would be precluded if undertaken as a valid countermeasure. A state is entitled to take countermeasures that are otherwise unlawful actions or omissions in response to an internationally wrongful act by another state under certain conditions.[212]

---

by kinetic weapons. For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. … Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force.").

[206] Kuschner, *supra* note 169.

[207] Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under international Law*, 64 A.F. L. Rev. 121 (2009).

[208] Koh, *supra* note 205.

[209] U.N. Charter, art. 2(4).

[210] Koh, *supra* note 205.

[211] Law of War, s*upra* note 105, at 1016.

[212] Edwin Djabatey, U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I: *Would Economic Cyber Intrusions Against U.S. Entities Violate International Law?*, Just Security (2019),

e. State Sovereignty

In our scenario, U.S. cyber actions against North Korea potentially involved malware insertion into launch and control systems. Assuming cyber operations to implant harmful malware violates sovereignty, a response in kind would need to qualify as a countermeasure under the law of state responsibility to be lawful. The requirements for countermeasures have been set forth by the International Law Commission in its Articles on State Responsibility,[213] which are generally considered to reflect customary international law. The key requirement is that the countermeasure of the "injured" state be intended to convince the "responsible" state to desist in its unlawful activities regarding emplacement of the malware. Countermeasures are also permissible to secure assurances, guarantees, or reparations. A guarantee may take the form of neutralization or removal of the malware in question. Additionally, unlike in self-defense, countermeasures may not be anticipatory in character, must be proportionate to the unlawful act to which they respond, and must not constitute a use of force.[214]

Transboundary cyber operations conducted by the military may implicate articles 2(4) and 51 of the United Nations Charter, which prohibit the threat or use of force by states except in unilateral or collective self-defense in the case of an "armed attack." For a cyber operation to be a use of force, it must be equivalent in scale and effect to a conventional use of force.[215] Mere emplacement of malware does rise to the level of a prohibited use of force in violation of Article 2(4) of the UN Charter and customary international law. As with the rule of sovereignty, there is uncertainty regarding the threshold at which the prohibition is breached by a hostile cyber operation. An operation that causes physical damage or injury beyond a de minimus level would reach that threshold. Arguably, so too would cyber operations having severe consequences, such as a cyber-attack with devastating effects on a nation's economic system, although this remains an open question among states.[216]

It is worth noting that cyber espionage, the collection of information vital to the protection of the state, does not breach international law, which is generally silent on the permissibility of states collecting intelligence on each other. This is due to widespread acceptance that all states engage in espionage to some degree. Generally, those matters that international law does not regulate are left to states' domestic legal orders to regulate.[217] [218]

According to the *Tallinn Manual*,[219] there is consensus that a cyber operation could breach the target state's sovereignty in two cases: 1) if it causes damage to cyber infrastructure in that state or interferes in a relatively permanent way with the functionality of such infrastructure (based on the premise that as the target state alone controls access to its sovereign territory, the causation of these effects without its

https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/.

[213] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (2001) https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

[214] Michael Schmitt, *U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply*?, Just Security (2019), https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/.

[215] Djabatey, *supra* note 212.

[216] Schmitt, *supra* note 214.

[217] *The Case of the SS Lotus*, 19 (1927), https://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf.

[218] Djabatey, *supra* note 212.

[219] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 20 (2nd ed. 2017), https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

consent amounts to a clear infringement of the target state's territorial integrity); and 2) if the cyber breach amounts to interference with or an usurpation of one of the target state's inherently governmental functions. As sovereignty guarantees the target state the exclusive right to exercise the functions of a state within its own territory,[220] any interference with this right would violate sovereignty.[221]

VIII. Space Assets and Critical Infrastructure

The discussion of how the U.S. might respond to a cyberattack on space-based critical infrastructure ultimately rests upon the nation's ability to adapt to complexity and uncertainty. The first point of clarification is to understand critical infrastructure as a complex system-of-systems for which policy has only recently formed to articulate its complexity and growing need for cybersecurity. In addition to weaknesses inherent in critical infrastructure due to design, legacy considerations, and environmental dependencies, the realization of diverse actors and worsening threat trends highlight the scale of the problem.[222]

a. Space Assets

A "space asset" is any man-made uniquely identifiable asset in space or designed to be launched into space, and comprising a spacecraft, such as a satellite, space station, space module, space capsule, space vehicle or reusable launch vehicle, whether or not including a space asset falling within (ii) or (iii) below:

> (ii) a payload (whether telecommunications, navigation, observation, scientific or otherwise) in respect of which a separate registration may be effected in accordance with the regulations; or (iii) a part of a spacecraft or payload such as a transponder, in respect of which a separate registration may be effected in accordance with the regulations, together with all installed, incorporated or attached accessories, parts and equipment and all data, manuals and records relating thereto."[223]

Satellites are an important example of space assets. With the increased capabilities and growing dependence on civil and military uses of satellites, their vulnerability to both natural and man-made threats is becoming apparent. The threat to satellites is posed by various types of weapons aimed at orbiting spacecraft and by increasing amounts of debris. Land- and space-based kinetic energy and some land-based laser weapons pose immediate threats to space assets.[224]

For decades there has been a strong correlation between space exploration efforts and the military and intelligence communities. Declassified Central Intelligence Agency (CIA) documents reveal that at least as early as 1977, the agency was concerned that "visible military support role for reconnaissance

---

[220] *The Island of Palmas Case (or Miangas) (United States of America v. The Netherlands)*, 8, https://pcacases.com/web/sendAttach/714.
[221] Djabatey, *supra* note 212.
[222] Scott A. Weed, *U.S. Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure*, 3 (2017). https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/CPP0007_WEED_SCADA.PDF.
[223] *Protocol to the Convention on International Interests in Mobile Equipment on Matters Specific to Space Assets* (2012), https://www.unidroit.org/instruments/security-interests/space-protocol.
[224] Bhupendra Jasani, *Space Assets and Emerging Threats* (2016), https://www.unoosa.org/pdf/SLW2016/Panel2/1_Jasani_-_Space_assets_and_threats_06082016.pdf.

satellites" would "increase the likelihood that they [would] become targets at certain levels of crises or conflicts."[225]

b. Critical Infrastructure and Assets

The USA PATRIOT Act of 2001, defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[226] Critical infrastructure and key resources (CI/KR) are "[t]he infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence."[227] A "critical asset" is "[a] specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.[228]

Some of the space sector functions within the defense infrastructure include space surveillance, ballistic missiles, tactical warning and attack assessment, and communications.[229] GPS is one of several systems, sub-systems, capabilities, and functions which has been identified as critical to the Department of Defense.[230] As a potential reason why this might be the case, the U.S. Army reportedly employed 100,000 precision GPS receivers[231] during Operation Iraqi Freedom, making the technology available down to the squad level.[232]

c. Government Risk Management Efforts and Response Capabilities

In August 2005, DoD established the Defense Critical Infrastructure Program (DCIP), which is a "DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.[233] In October 2008, DoD formalized the process for identifying and prioritizing its critical infrastructure. To support the effort, combatant commands and military services identified and placed their critical assets into prioritized tiers. Tier 1 Task Critical Assets are assets whose incapacitation or destruction would have a debilitating effect on the ability of one or more military services, combatant commands, or DCIP Defense Infrastructure Sector Lead Agents to execute mission essential tasks.[234] The Government Accountability Office (GAO) reported that because DoD lacks

---

[225] Central Intelligence Agency memo CIA-RDP83M00171R001000190001-6, *Tactical Use of Reconnaissance Satellite Assets*, 94 (1977), https://www.cia.gov/library/readingroom/docs/CIA-RDP83M00171R001000190001-6.pdf.

[226] USA PATRIOT Act of 2001 § 1016, 42 U.S.C. § 5195c(e) (2006).

[227] Joint Publication 3-27, *Homeland Defense* (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf.

[228] Joint Publication 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism* (2014).

[229] Department of Defense Manual 3020.45, Volume 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*, Enclosure 6, 23 (2008), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V1p.pdf.

[230] *Id*. at 9.

[231] AN/PSN-11 Precision Lightweight GPS Receiver (PLGR, or "Plugger") is a ruggedized, handheld, single-frequency GPS receiver that incorporates the Precise Positioning Service Security Module (PPS-SM) to access the encrypted P(Y)-code GPS signal.

[232] Seth Schiesel, *On the Ground in Iraq, the Best Compass Is in the Sky*, N.Y. Times (2003), https://www.nytimes.com/2003/04/17/technology/on-the-ground-in-iraq-the-best-compass-is-in-the-sky.html.

[233] Department of Defense Directive 3020.40, *Mission Assurance (MA)* (2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983.

[234] Government Accountability Office GAO-09-740R, *Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List* (2009), https://www.gao.gov/products/GAO-09-740R.

a formal process for submitting critical assets, the combatant commands and military services are limited in their ability to effectively select, compile, and validate their final nominations to DoD's Tier 1 Task Critical Asset list.[235]

According to Presidential Policy Directive (PPD) 21, critical infrastructure must be "secure and able to withstand and rapidly recover from all hazards" and depends on complex "distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations."[236] The directive specifically identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.[237]

The incipiency of cyberspace and the difficulty of calculating and delivering cyber effects generates concern that errant cyber activity might degrade or disrupt international and dual-use cyberspace and generate negative strategic effects.[238] Accurate and consistent use of mitigative counterstrikes could serve to deter cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure (CNI). Supporters argue that implementing a regime to permit these sorts of counterattacks should be a priority.[239] The U.S. is one of only a few nations which has claimed an offensive cyber capability, ostensibly to dissuade adversaries through the assurance that the U.S. retains freedom of action across a full spectrum of response options. The principle that any response to cyber incidents will be the minimum sufficient force required to achieve the desired effect is central to U.S. cyber policy and reiterated across the other federal directives and in law. This emphasis on restraint provides law enforcement options and countermeasures be exhausted and determined to be insufficient before cyber options are considered.[240]

d. Space Assets as Critical Assets

Given that United States Space Command (USSPACECOM) is a unified combatant command responsible for military operations in outer space, that combatant commands are tasked with identifying critical assets, and that communications systems have been identified as being uniquely critical, one can assume (although the list is classified) that some space-based assets and systems have been designated as critical infrastructure and likely reside on the Tier 1 Task Critical Asset list.

The military is built on redundancy, the theory being that the military should still be able to function even if a certain percentage of equipment becomes inoperable or is destroyed in combat. However, some systems are so expensive or unique that redundancy is not possible, and destruction of these systems would severely hamper the ability of the U.S. to defend itself. For example, missile warning satellites operate at higher orbital altitudes and use infrared sensors to detect heat sources on the surface of the earth and above it. The hot plume exiting a rocket engine is detected by satellites, and the intensity and length of a rocket engine's burn and trajectory allow ground stations to determine the

[235] *Id*.

[236] Barack H. Obama, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[237] Weed, *supra* note 222.

[238] *Id*. at 15.

[239] Koh, *supra* note 205, at 415, 421.

[240] Weed, s*upra* note 222 at 24-25.

range and type of the rocket. This also enables classification of the rocket type: missile or space booster. Analyzing all this information about the rocket, an assessment is made on whether an attack is in progress and whether early warning radars and missile defenses should be cued. Early warning enabled by these satellites provides the President and operational commanders the maximum time possible to prepare for and respond to an attack. Without these space assets, warning times would be limited to the much shorter timelines achievable with the coverage of missile warning radars alone,[241] which could result in disaster.

IX. Conclusion

While freedom of action is generally desirable and has led to greater opportunity and prosperity for smaller nation states, an increasing reliance on space systems for national security and the simultaneous emergence of counterspace capabilities is making the space domain more competitive and contested than ever before.[242] Space is a naturally hazardous environment and is becoming increasingly congested, contested, and competitive. The increasing weaponization of outer space poses not only difficult legal questions but also represents a clear and present danger to international peace and security.[243] International law has codified limits for the sovereign dimensions of land, sea, and air while conventional law has sought to limit space by purpose or intent. Since space overlays other environments, even those nations unable to launch satellites hold it in high regard. Conventional law awaits customary judgment as to whether outer space is an international free regime, akin to the high seas and international airspace, or one restricted to benevolent use. Like space, information is a pervasive medium, and rapid development of computer technology and inexpensive operating costs may cause technology to transcend legal precedents.[244] Space and cyber laws and principles are merging as the operation of satellites and other space assets relies on internet-based networks.[245]

Both strategically and operationally, the military is still grappling with the convergence of electronic warfare and cyber warfare as well as the integration of the two. It should be noted that electronic warfare has not yet completely absorbed cyber warfare. The Army, for example, has moved toward the fusion of the two but, to date, EW and cyber operational planners continue working to deconflict each other's operations.[246]

The rise of great-power competitors such as China and Russia have prompted the U.S. military to transform the way it plans to fight in the multiple domains of cyber and space. The expanded battlefield now stretches far beyond the front lines or close areas where ground forces traditionally face off against

---

[241] William L. Shelton, Statement Before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications, Threats to Space Assets and Implications for Homeland Security, 4 (2017), https://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf.

[242] UNIDIR Space Dossier 3, *Electronic and Cyber Warfare in Outer Space* (2019), https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

[243] Jackson N. Maogoto & Steven Freeland, *Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?*, The International Lawyer, Vol. 41, No. 4, 1021-1119 (2007), http://www.jstor.org/stable/40707832.

[244] Karl J. Shawhan, *Vital Interests, Virtual Threats: Reconciling International Law with Information Warfare and United States Security*, 9-17 (2001), http://www.jstor.org/stable/resrep13990.8.

[245] David Fidler, *Cybersecurity and the New Era of Space* Activities, Council on Foreign Relations (2018), https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

[246] Michael Lilienthal personal correspondence, *EW Paper Comments* (2020).

each other. In the expanded battlefield, adversaries can use more sophisticated weapons and cyber capabilities based in distant and protected territories, potentially reaching targets that are located well behind the front lines, even within the continental United States.[247]

The U.S. must use every tool at its disposal to discourage potential space rivals from inflicting damage on critical space assets and must respond quickly in kind to threats. To the extent that electronic and cyber warfare can be waged without injury or human suffering, this is preferred. But war in all forms has the potential for casualties. Merely because a hostile act takes place via the Internet or in the far reaches of space does not make the act any less hostile. The U.S. should expand not only the range but the spectrum of possible threat responses, and robust cyber and electronic warfare capabilities continue to prove their worth in the face of expanding threats.

[247] See GAO-19-570, *Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New* (2019), https://www.gao.gov/assets/710/700940.pdf.